Study Group Workshop 2026　成果報告集
課題提供：株式会社インターネットイニシアティブ
SGW2026

PQC時代の暗号資産鍵管理における安全性・可用性・運用コストのトレードオフの定量評価

編集者）
倉田 澄人（九州大学マス・フォア・インダストリ研究所）
今村 浩二（九州大学マス・フォア・インダストリ研究所）
金重 幸大（九州大学大学院マス・フォア・イノベーション連係学府）
山崎 拓己（九州大学大学院マス・フォア・イノベーション連係学府）

この成果報告集について

- 成果報告集は複数の成果報告書をまとめたものです
  - ✓ 成果報告書の下線付きの著者は、成果報告会（SGW5日目）で登壇したことを表します
  - ✓ 登壇の有無に関わらず、成果報告書を成果報告集に採用することがあります

- 著作権および利用条件について
  - ✓ 含まれる成果物の著作権は、原則として各成果物の創出者に帰属します
  - ✓ 閲覧および閲覧・参照を目的としたダウンロードは自由です
  - ✓ これらを超える転載、複製、改変、再配布、公衆送信等の自由利用の直接の対象は、原則としてSGW構成員です
    - 第三者による利用は、著作権法上認められる場合、または権利者・SGW構成員等の許諾がある場合に限られます
    - 製品開発等の商業的利用は、自由利用の対象外です
  - ✓ 記載されたSGW2026由来のアイデアやノウハウそのものは、第三者も無償で自由に利用できます
  - ✓ 詳細は以下のSGW規約をご確認ください
    - 国立大学法人九州大学マス・フォア・インダストリ研究所 スタディグループ・ワークショップ規約

© 2026 Respective authors / creators.

目次

- 課題説明
  - ✓ 金重 幸大（九州大学マス・フォア・イノベーション連係学府）
- マルチシグ(Multi-sig)に対するしきい値t/nの最適設計
  - ✓ 山崎 拓己（九州大学大学院マス・フォア・イノベーション連係学府）
  - ✓ 安田 渓（九州大学大学院マス・フォア・イノベーション連係学府）
  - ✓ 宮崎 雅哉（九州大学大学院マス・フォア・イノベーション連係学府）
  - ✓ 川西 晴貴（九州大学大学院数理学府）
- しきい値t/nの最適設計
  - ✓ 金重 幸大（九州大学大学院マス・フォア・イノベーション連係学府）
  - ✓ 朝重 菜音（九州大学大学院マス・フォア・イノベーション連係学府）
  - ✓ 村上 真悟（九州大学大学院マス・フォア・イノベーション連係学府）
  - ✓ 寺本 優斗（九州大学大学院数理学府）
  - ✓ 堂後 航希（九州大学大学院数理学府）

目次

- ホット・コールド分布の最適化
  - ✓ 山崎 拓己（九州大学大学院マス・フォア・イノベーション連係学府）
  - ✓ 安田 渓（九州大学大学院マス・フォア・イノベーション連係学府）
  - ✓ 宮崎 雅哉（九州大学大学院マス・フォア・イノベーション連係学府）
  - ✓ 川西 晴貴（九州大学大学院数理学府）

課題提供者、モデレーター等

- 課題提供者
  - ✓ 須賀 祐治（株式会社インターネットイニシアティブ ）
- コーディネーター
  - ✓ 縫田 光司（九州大学マス・フォア・インダストリ研究所）
  - ✓ 池松 泰彦（九州大学マス・フォア・インダストリ研究所）
- モデレーター
  - ✓ 倉田 澄人（九州大学マス・フォア・インダストリ研究所）
  - ✓ 今村 浩二（九州大学マス・フォア・インダストリ研究所）
- 学生モデレータ―
  - ✓ 金重 幸大（九州大学大学院マス・フォア・イノベーション連係学府）
  - ✓ 山崎 拓己（九州大学大学院マス・フォア・イノベーション連係学府）

課題説明

著者）
金重 幸大（九州大学大学院マス・フォア・イノベーション連係学府）

※朝重 菜音（九州大学大学院マス・フォア・イノベーション連係学府）が代理で発表

暗号資産とは

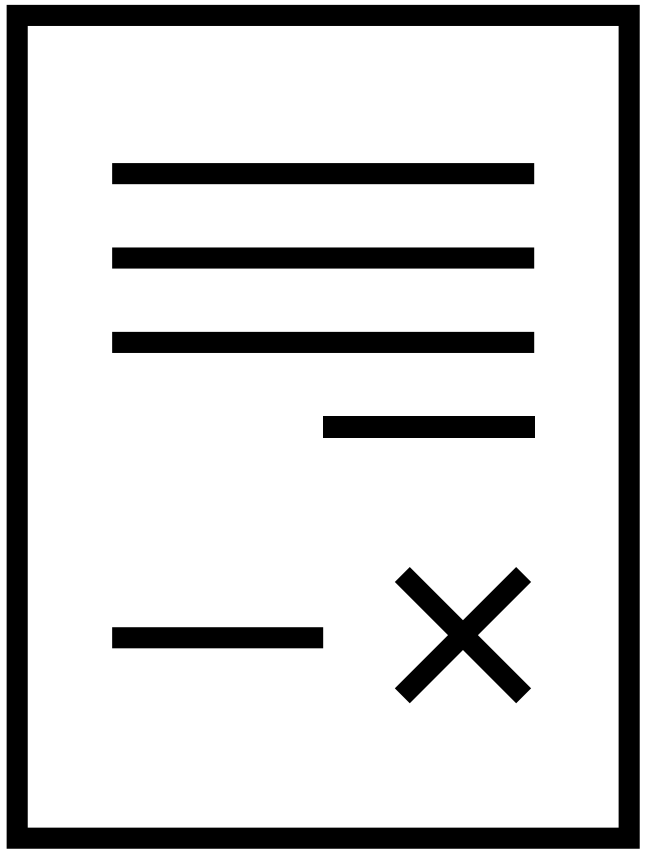
暗号資産とは、インターネット上でやり取りするデジタルな資産である。

暗号資産の取引

暗号資産の取引

暗号資産の取引

暗号資産の取引



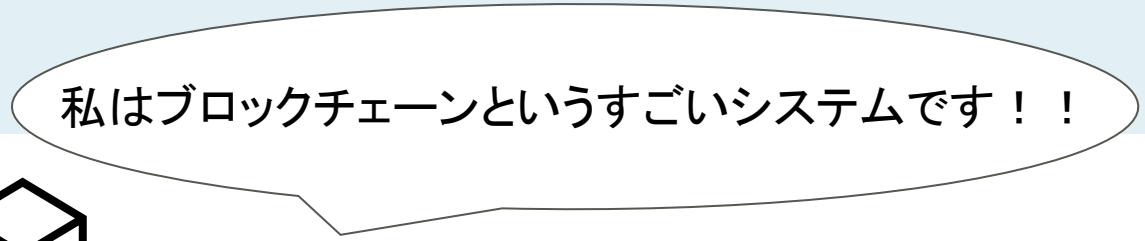
そうきんしゃ君は

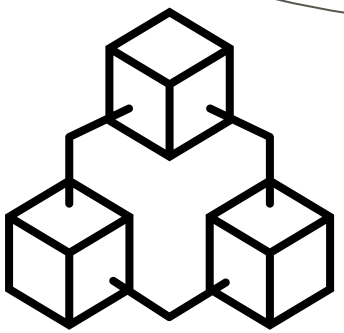
【『そうきんしゃ』は『うけとりのひと』に
〇〇円送る】

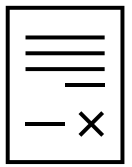
という文章（トランザクション）を作る。

暗号資産の取引

暗号資産の取引



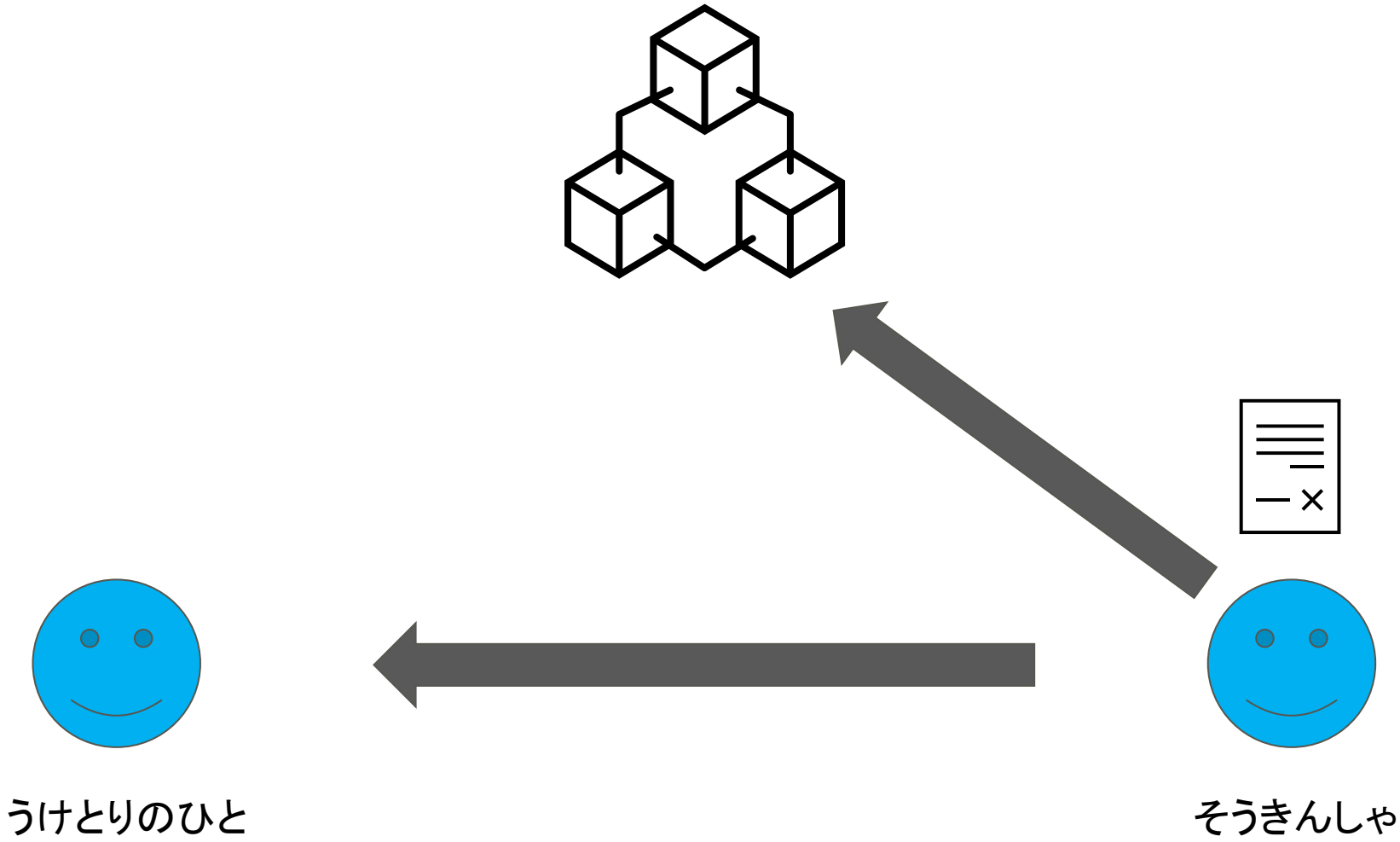




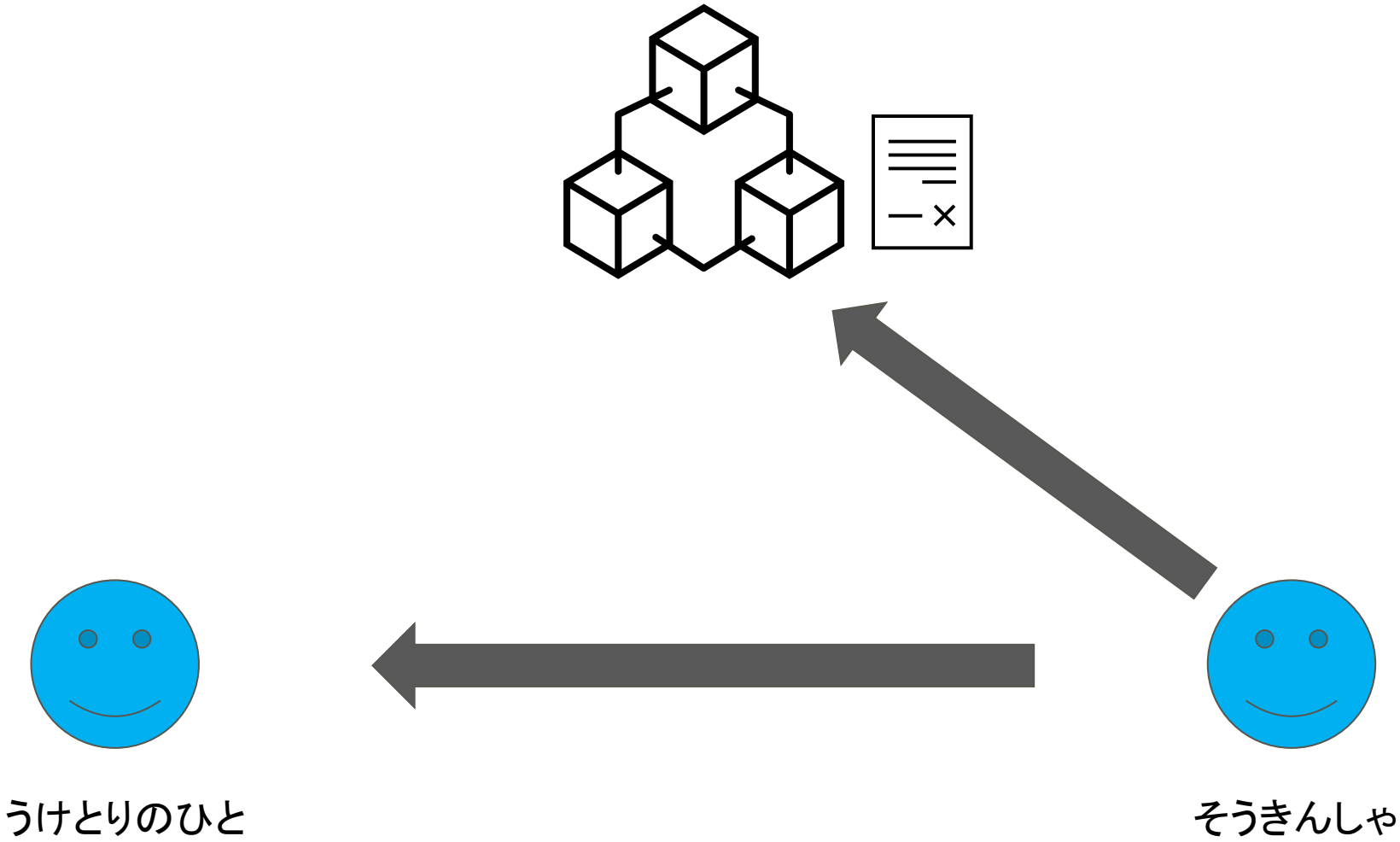
うけとりのひと

そうきんしゃ

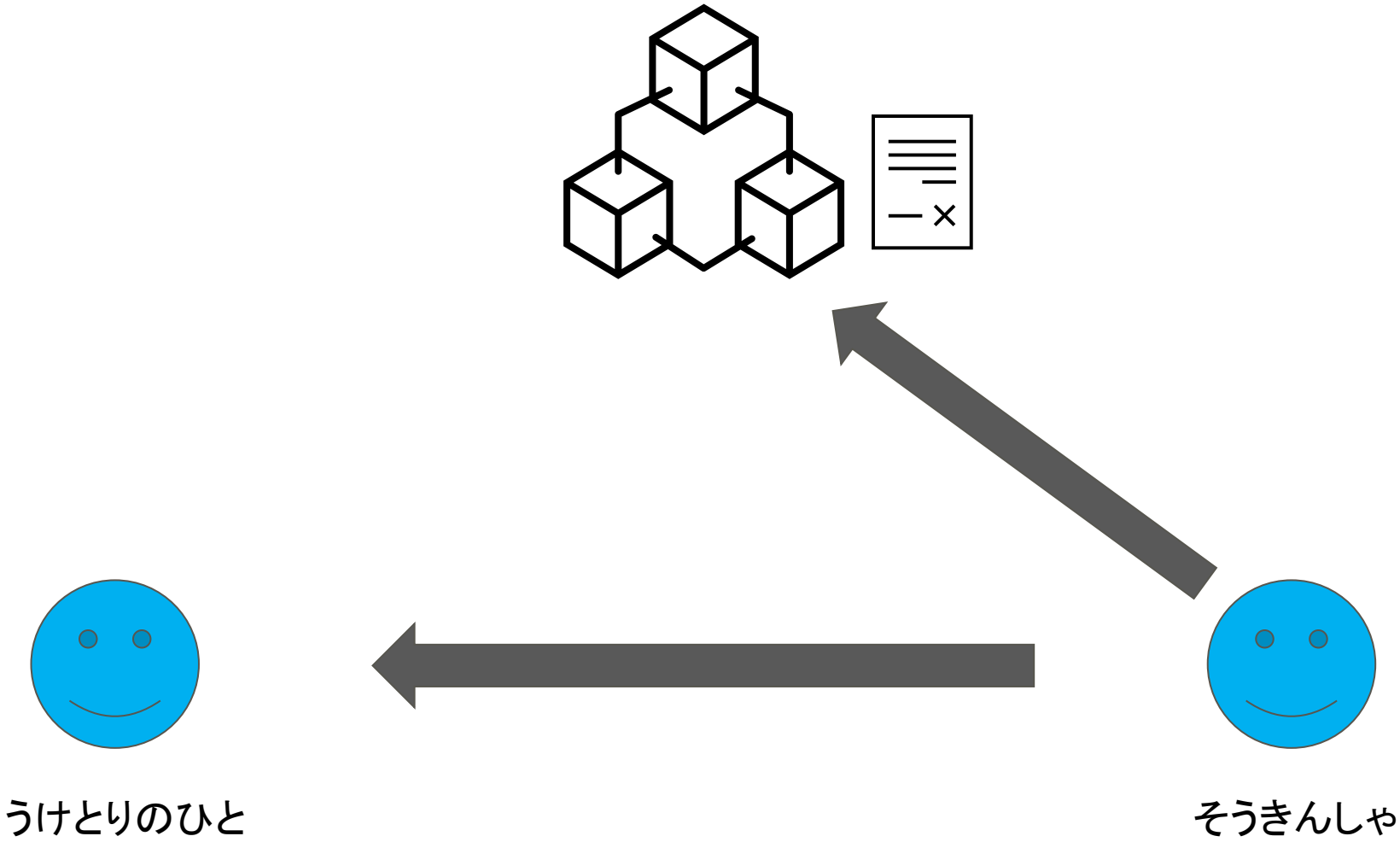
暗号資産の取引



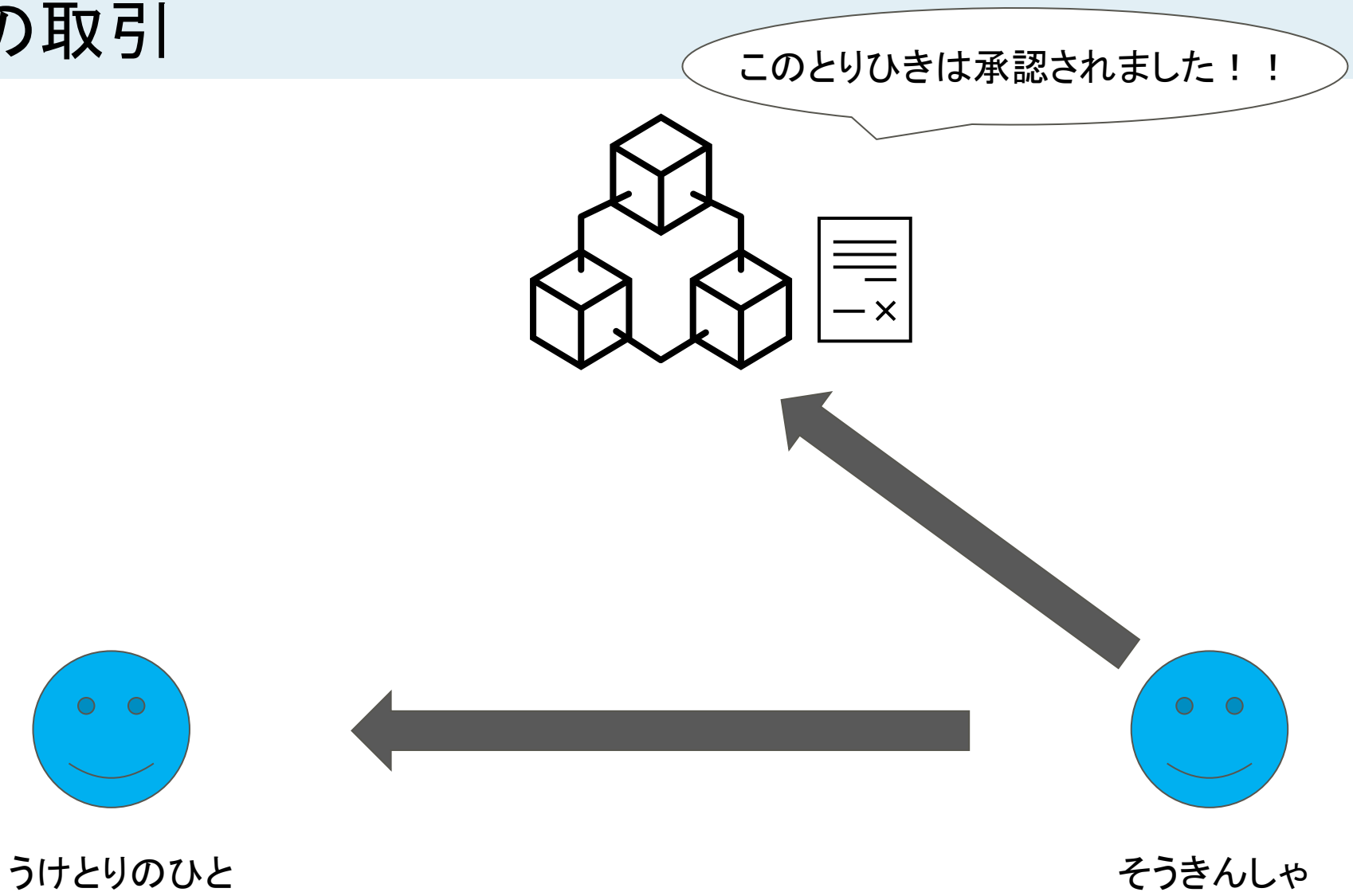
暗号資産の取引



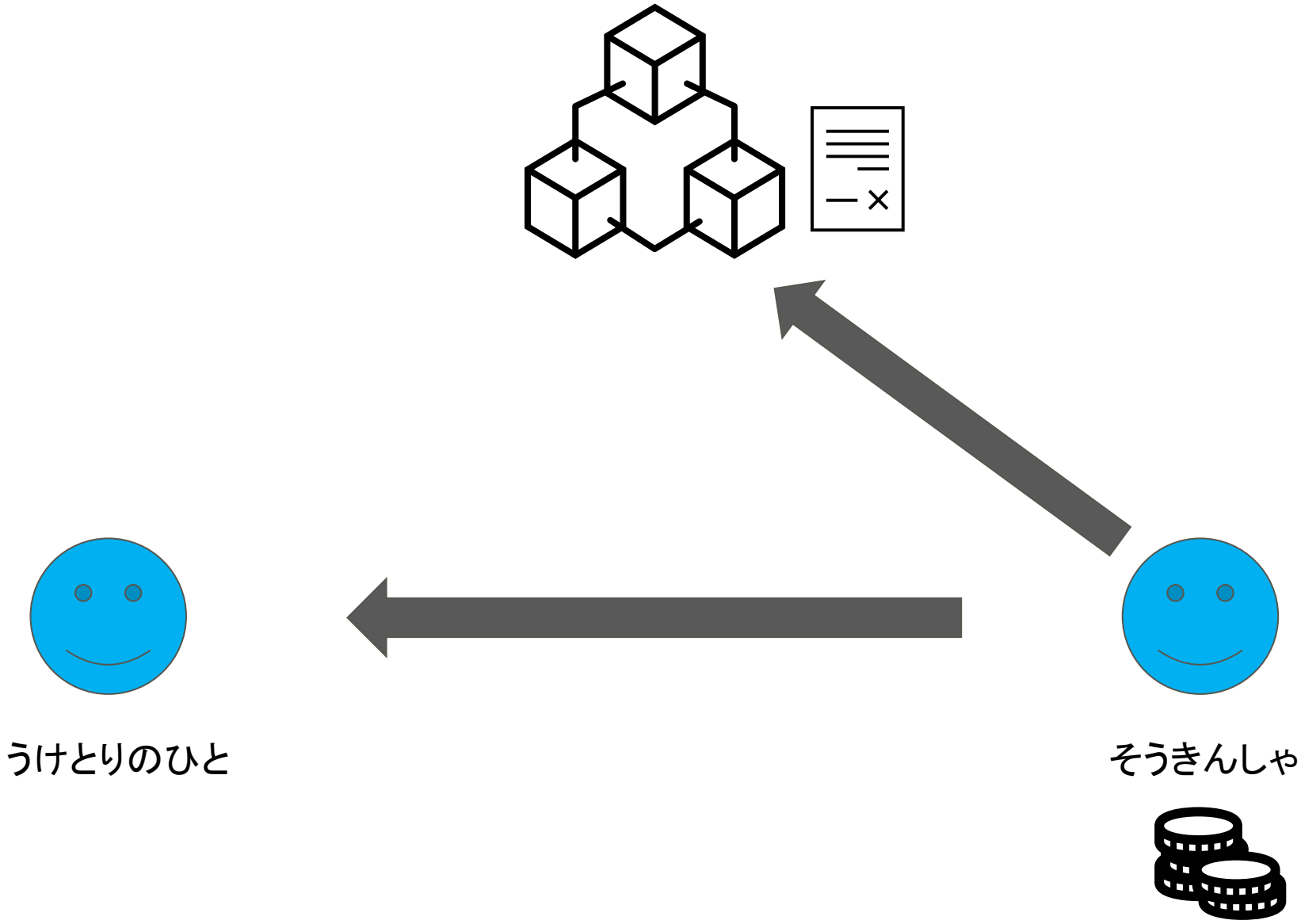
暗号資産の取引



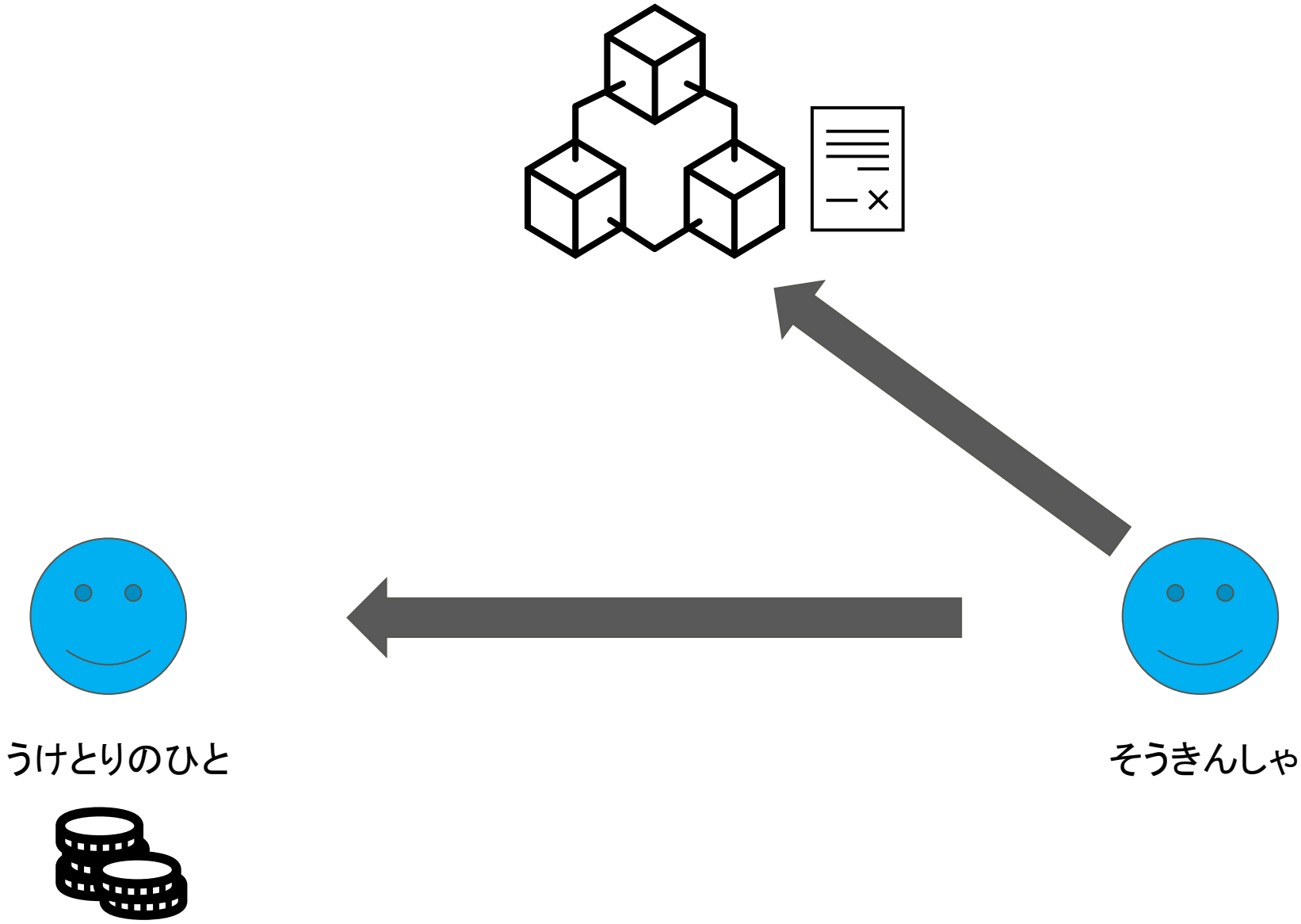
暗号資産の取引



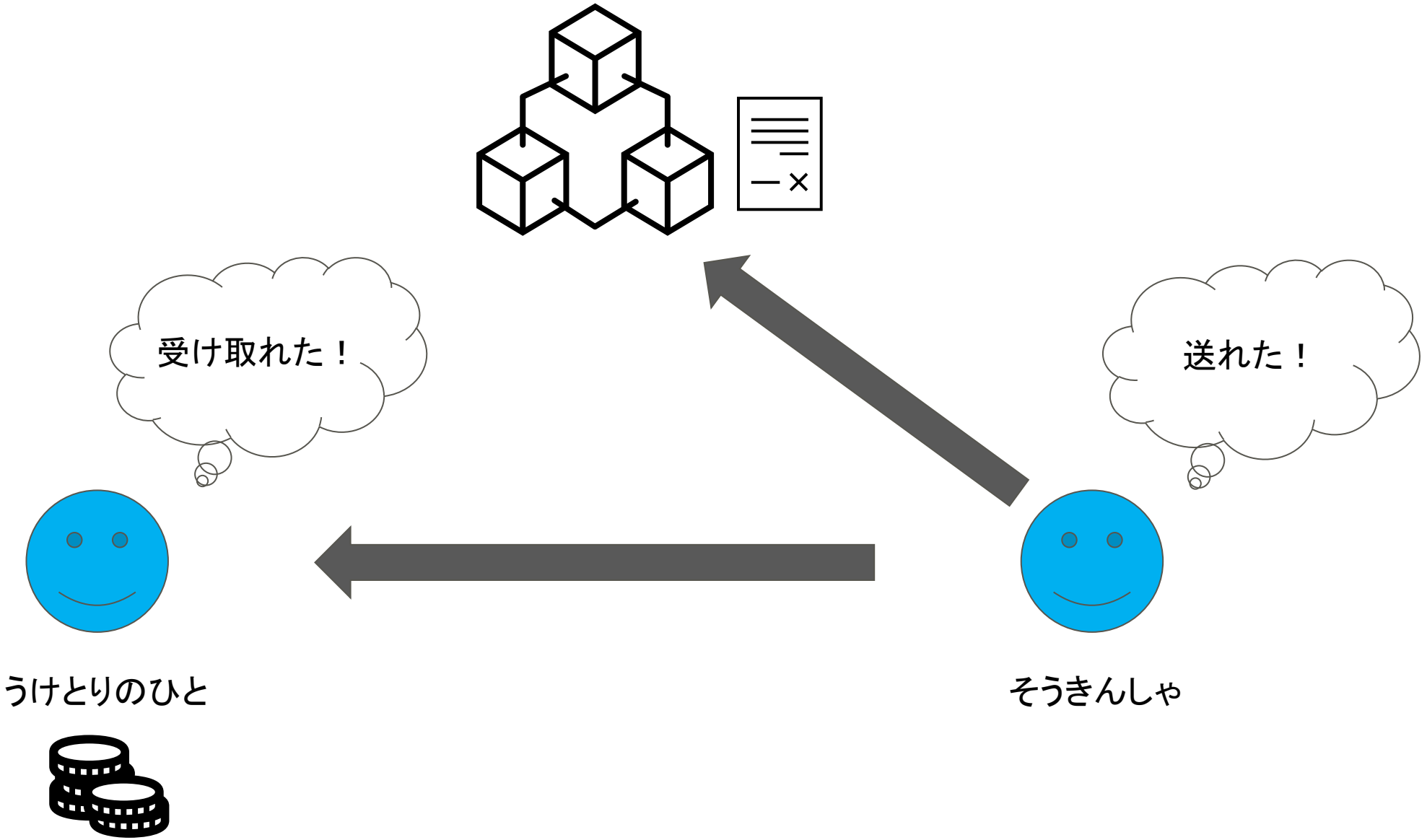
暗号資産の取引



暗号資産の取引



暗号資産の取引

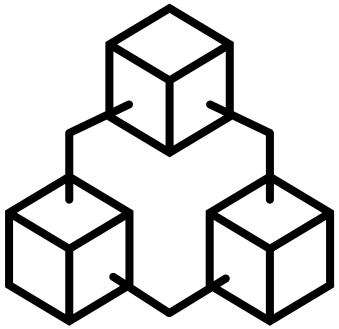


暗号資産の取引

簡単に言えば、ブロックチェーンというすごいシステムに
承認された取引のみが成立する

しかし、これから示すような問題点がある

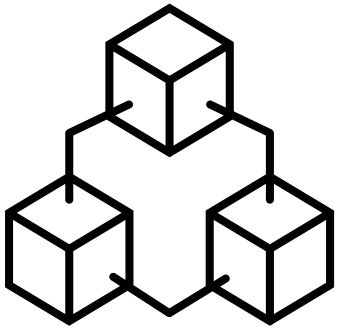
暗号資産の取引の問題点



わるいひと

そうきんしゃ

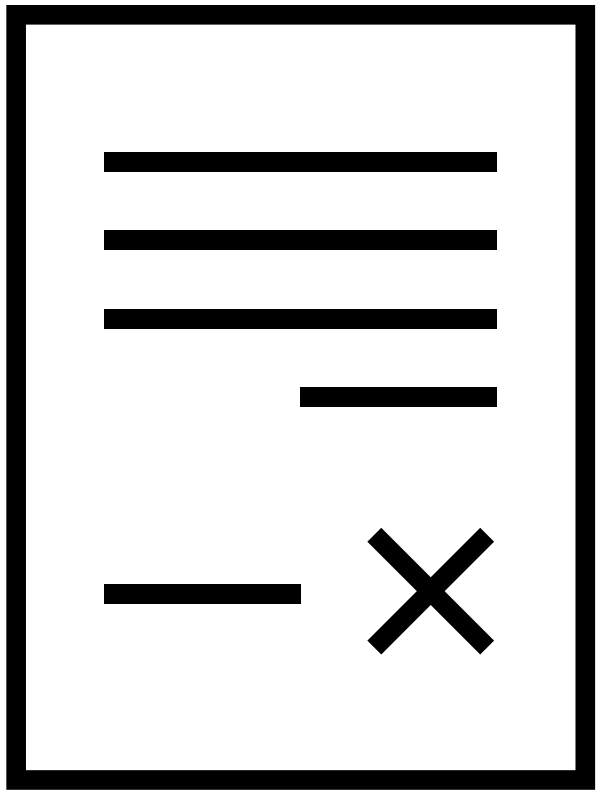
暗号資産の取引の問題点



わるいひと

そうきんしゃ

暗号資産の取引の問題点

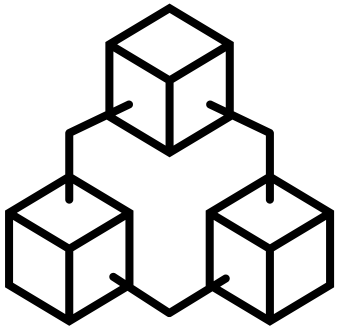


わるものくんが

【『そうきんしゃ』は『わるもの』に〇〇円送る】

というトランザクションを作る

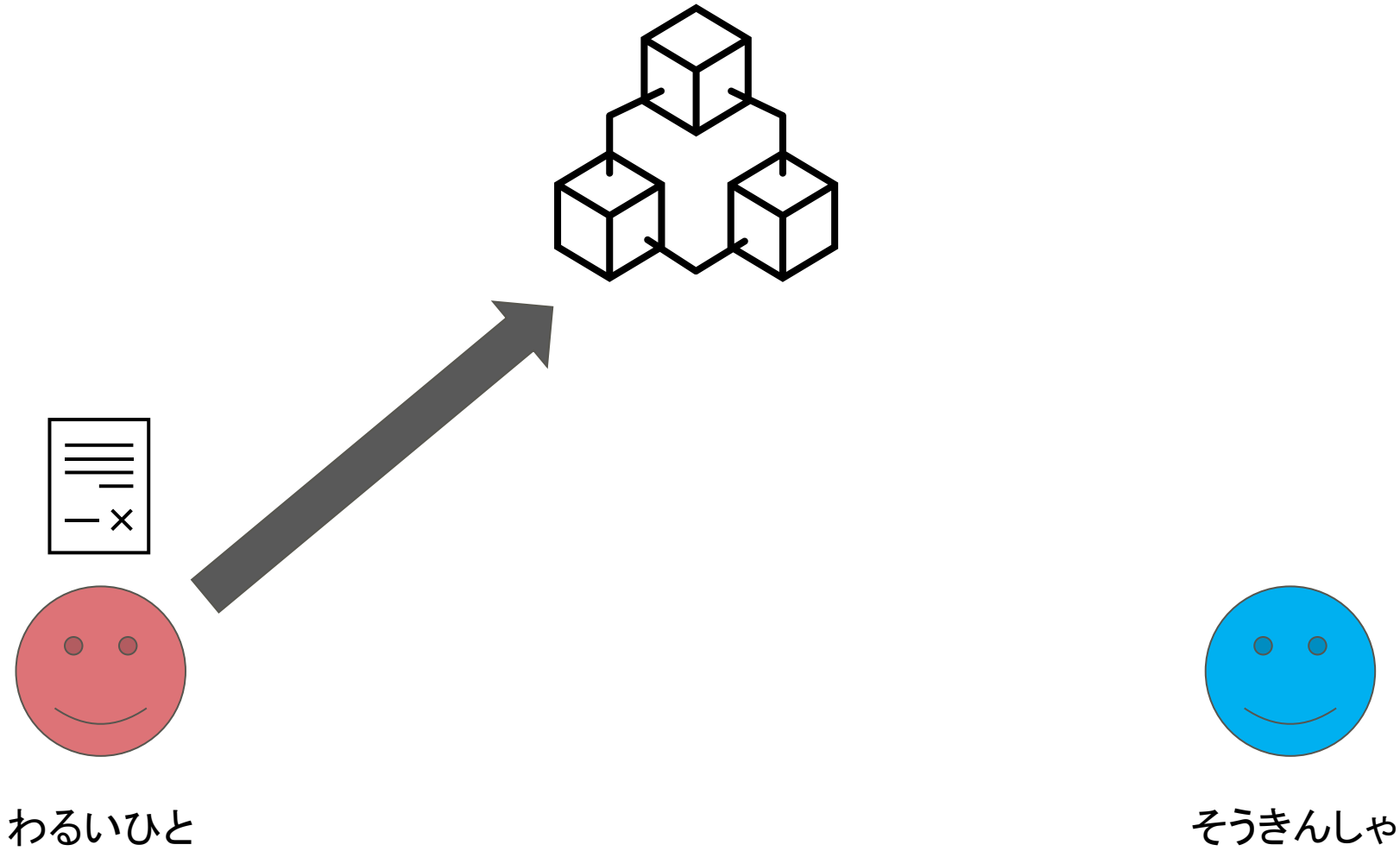
暗号資産の取引の問題点



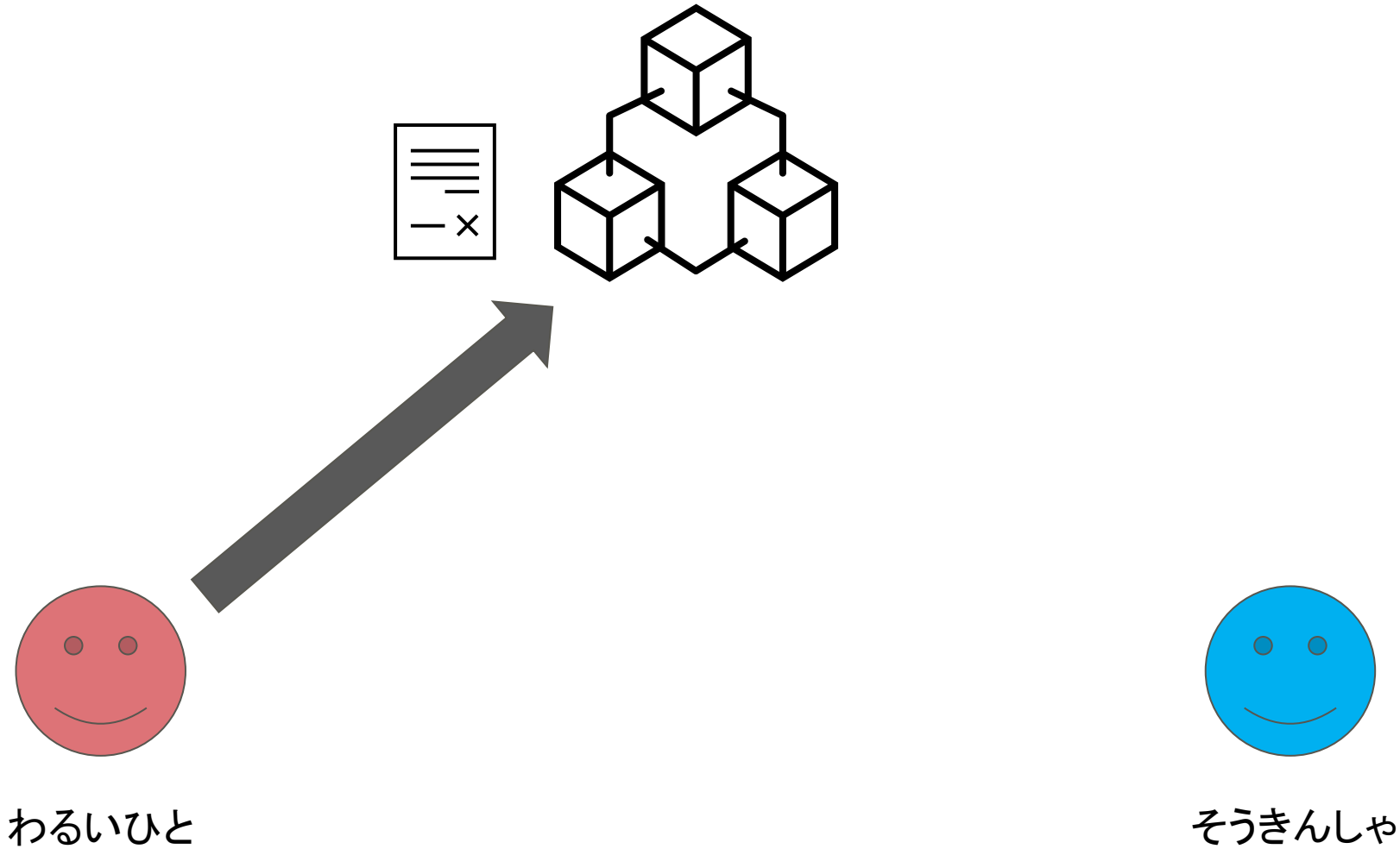
わるいひと

そうきんしゃ

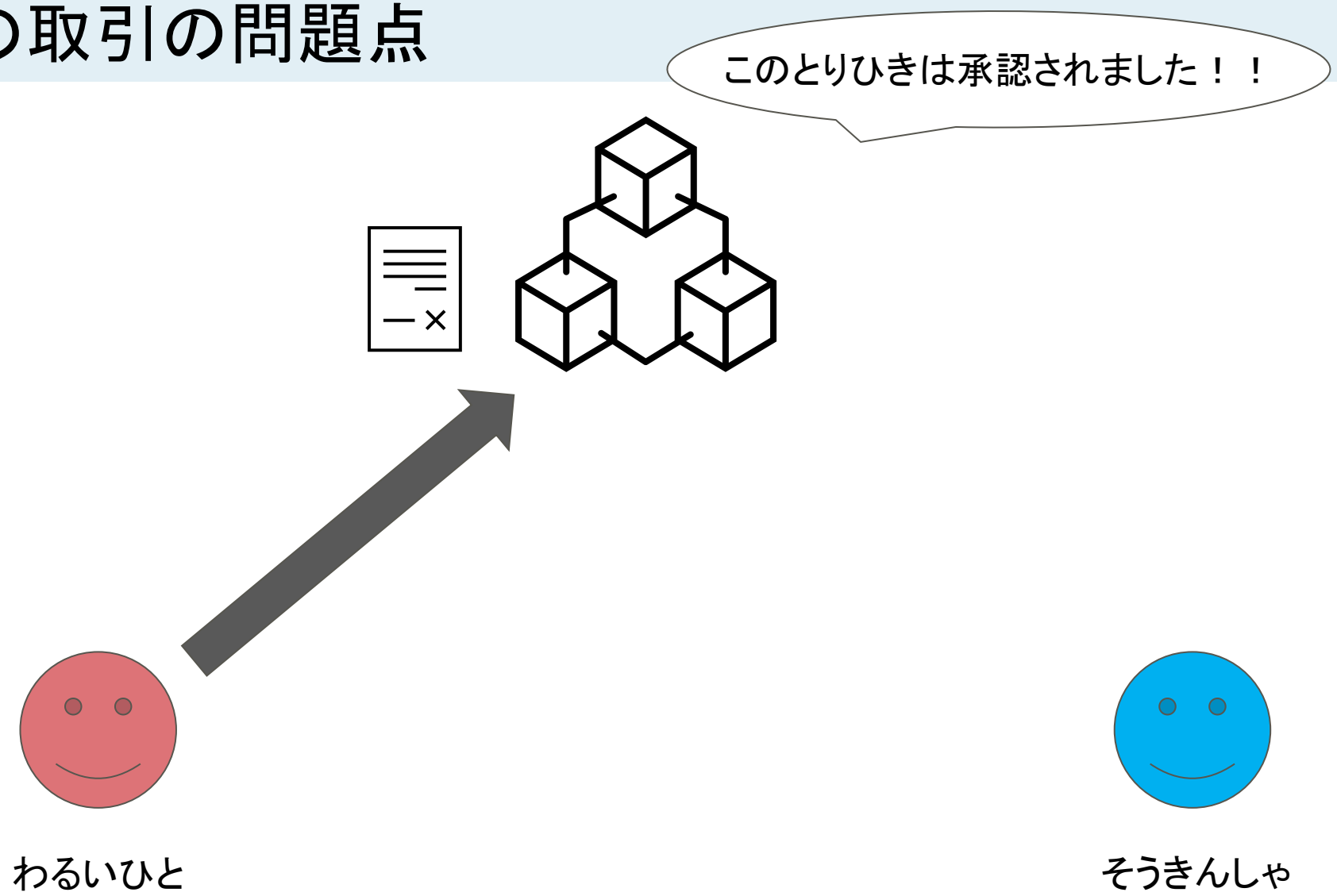
暗号資産の取引の問題点



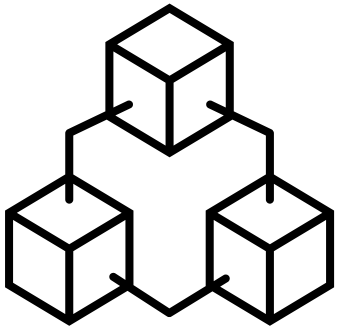
暗号資産の取引の問題点



暗号資産の取引の問題点

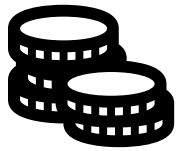


暗号資産の取引の問題点

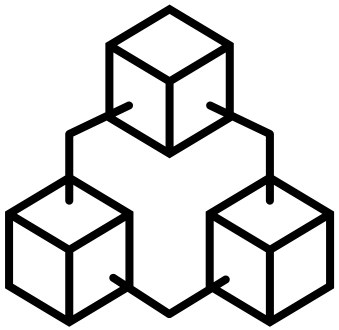


わるいひと

そうきんしゃ



暗号資産の取引の問題点

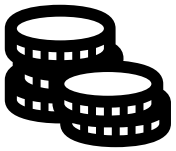


お金を奪えたぞ！！

お金が奪われた、、、

わるいひと

そうきんしゃ



暗号資産の取引の問題点

つまり、他人になりすまして、お金を移動することができてしまう。

これを解決するためには、文章（トランザクション）を書いた

ひとがそうきんしゃ本人であることを検証できなければならない

それを行うのがこれから示す電子署名というシステムである。

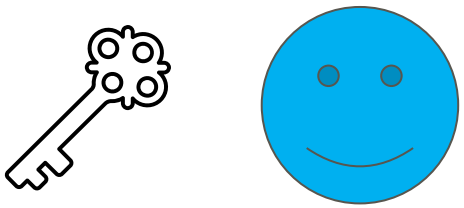
電子署名と鍵

暗号理論により、本当に持ち主が送ったものであるかを検証する方法がある。

これを電子署名という。

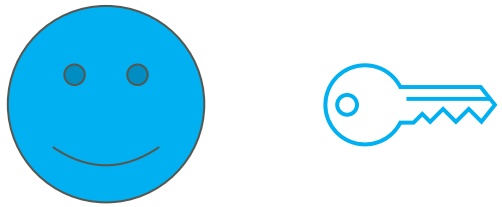
電子署名と鍵

検証鍵（公開）



けんしょうしゃ

署名鍵（秘密）



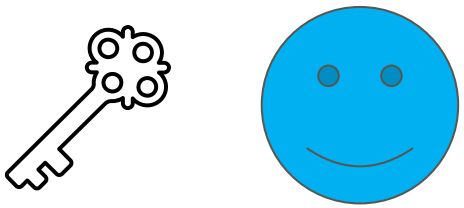
そうきんしゃ

電子署名と鍵

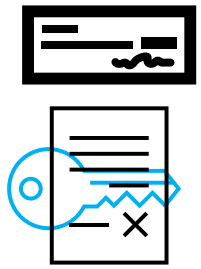
電子署名と鍵

電子署名と鍵

検証鍵（公開）



けんしょうしゃ



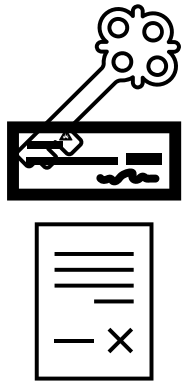
署名鍵（秘密）

そうきんしゃ

電子署名と鍵

電子署名と鍵

電子署名と鍵



検証鍵（公開）

署名鍵（秘密）

けんしょうしゃ

そうきんしゃ

電子署名と鍵

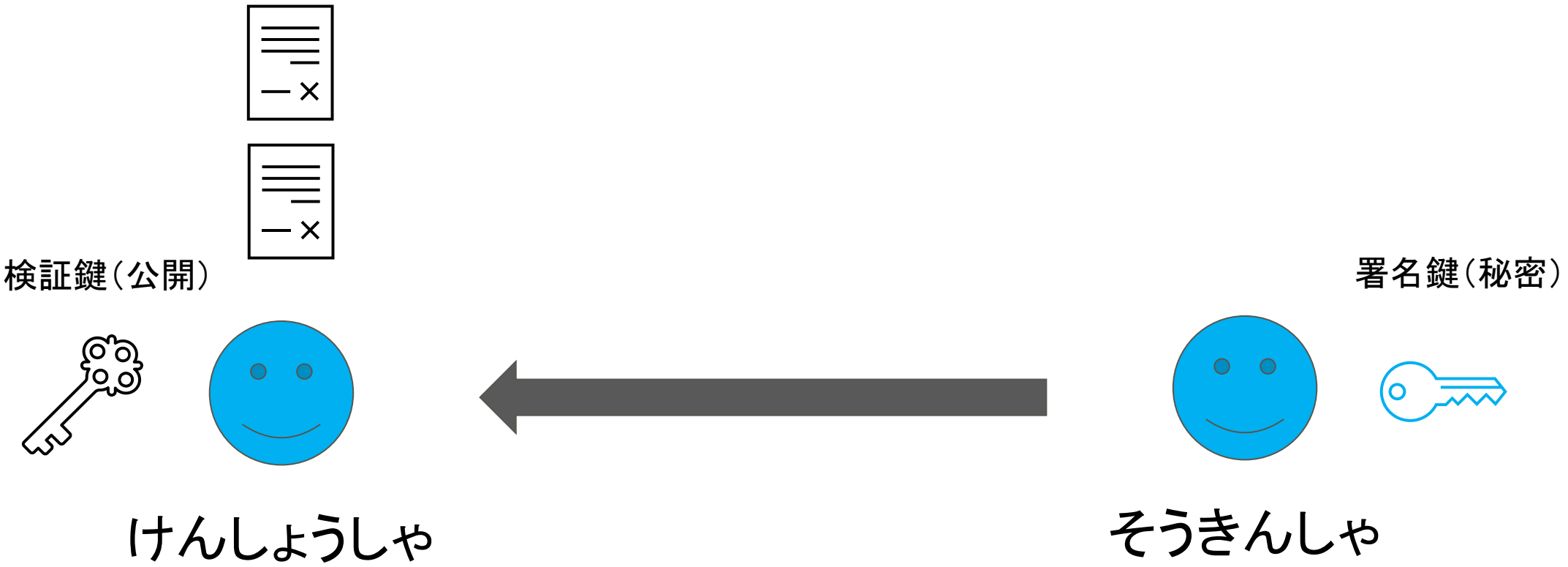
検証鍵（公開）

署名鍵（秘密）

けんしょうしゃ

そうきんしゃ

電子署名と鍵



電子署名と鍵

電子署名と鍵

電子署名と鍵

けんしょうしゃ

電子署名と鍵

けんしょうしゃ

電子署名と鍵

けんしょうしゃ

電子署名と鍵

検証鍵（公開）

けんしょうしゃ

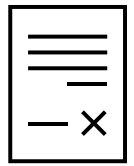
偽物署名鍵

わるもの

電子署名と鍵

検証鍵（公開）

けんしょうしゃ



偽物署名鍵

わるもの

電子署名と鍵

検証鍵（公開）

けんしょうしゃ

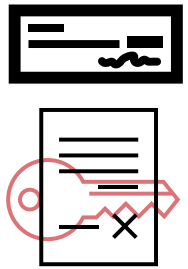
偽物署名鍵

わるもの

電子署名と鍵

検証鍵（公開）

けんしょうしゃ

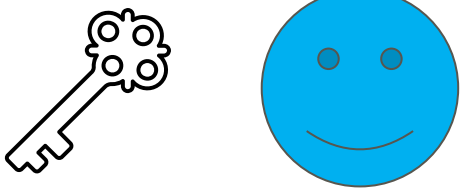


偽物署名鍵

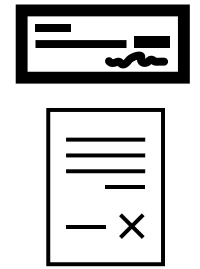
わるもの

電子署名と鍵

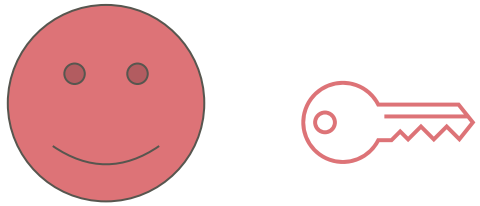
検証鍵（公開）



けんしょうしゃ



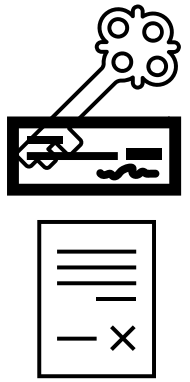
偽物署名鍵



わるもの

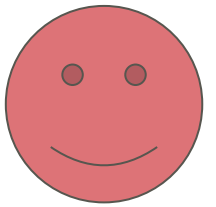
電子署名と鍵

電子署名と鍵



検証鍵（公開）

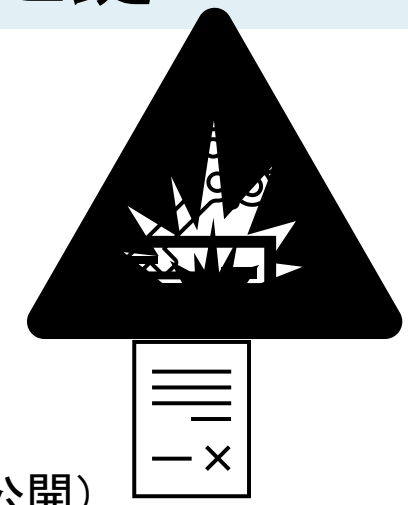
偽物署名鍵



けんしょうしゃ

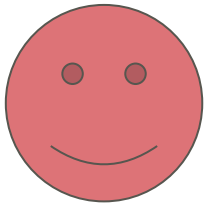
わるもの

電子署名と鍵



検証鍵（公開）

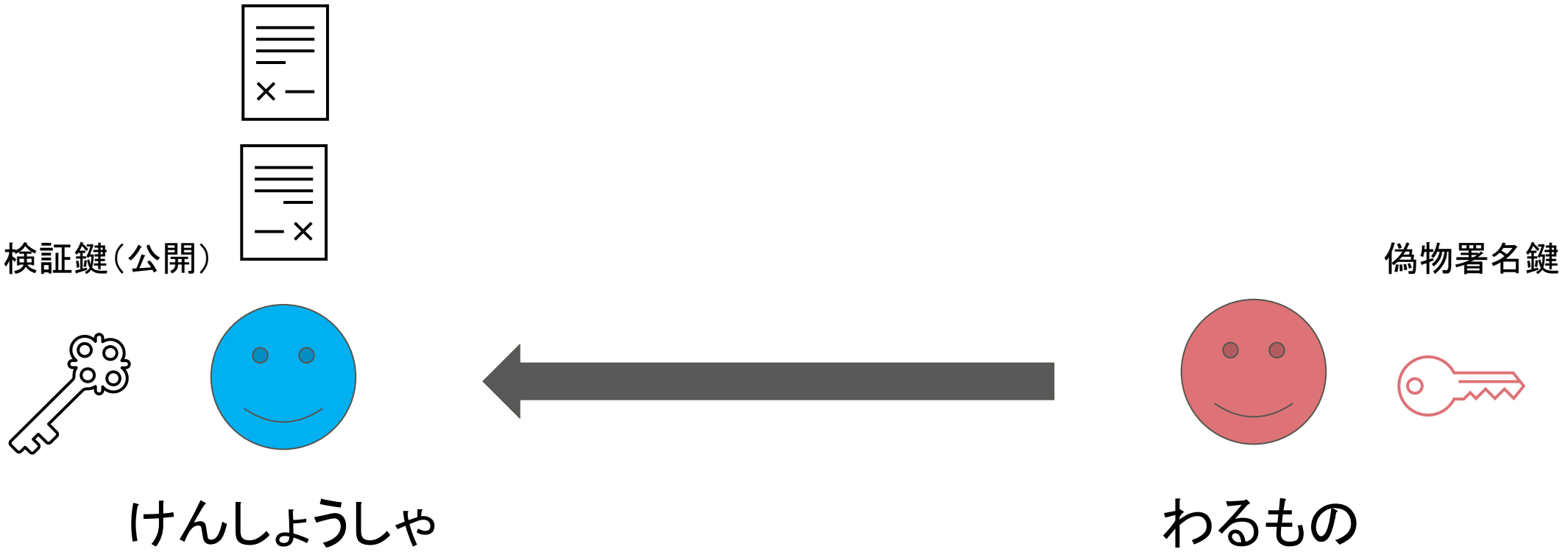
偽物署名鍵



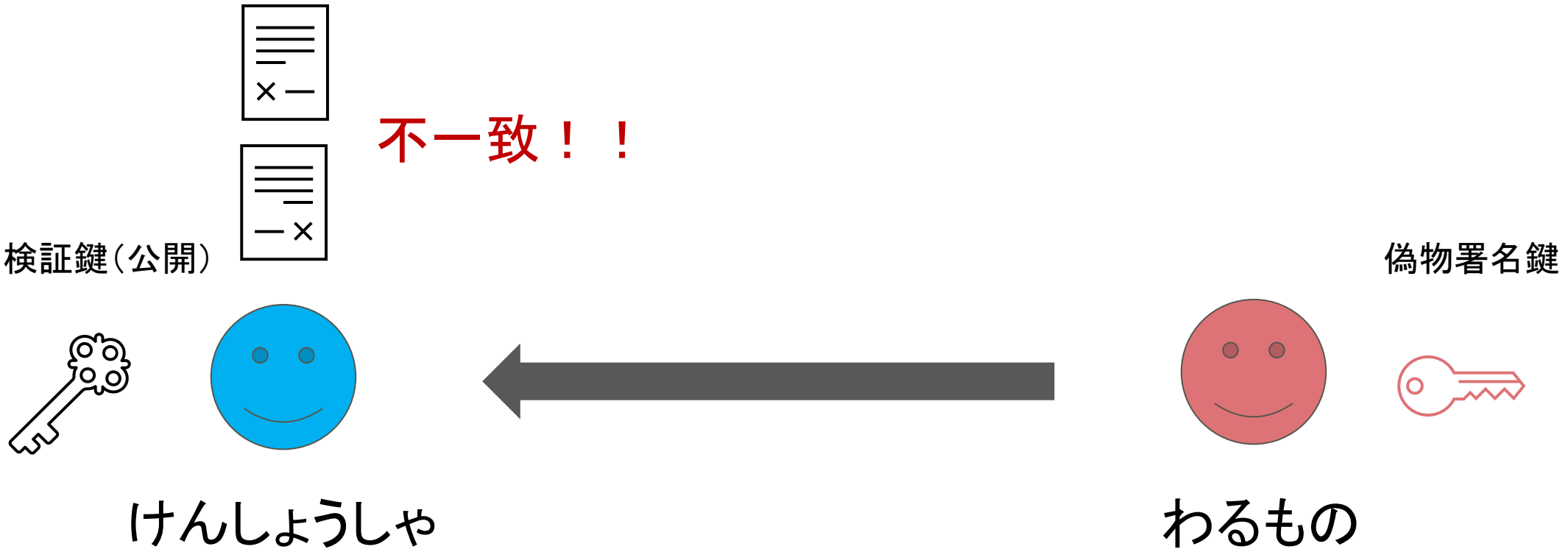
けんしょうしゃ

わるもの

電子署名と鍵



電子署名と鍵



電子署名と鍵

けんしょうしゃ

電子署名と鍵

けんしょうしゃ

電子署名と鍵

けんしょうしゃ

電子署名と鍵

つまり、トランザクションを誰が作成したかを判定する方法が与えられたことになる。

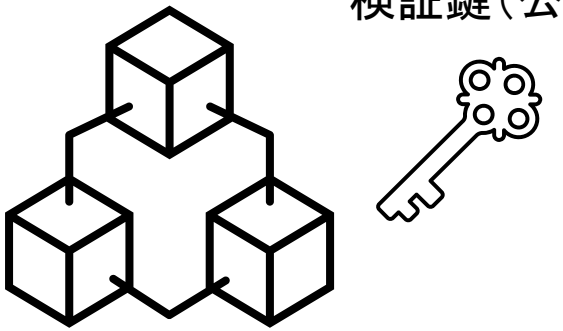
これにより「なりすまし」ができなくなる。

もし、署名鍵を奪われてしまったら、、、

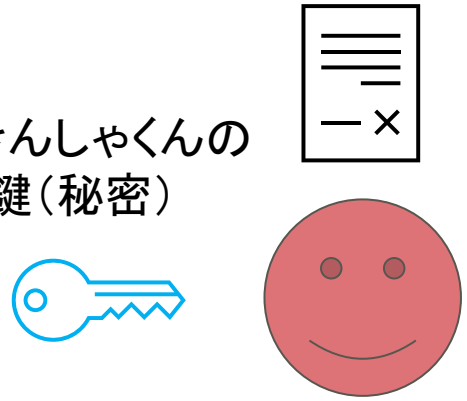
しかし、もし署名鍵が奪われてしまうと、、、

もし、署名鍵を奪われてしまったら、、、

検証鍵（公開）



そうきんしゃくんの
署名鍵（秘密）

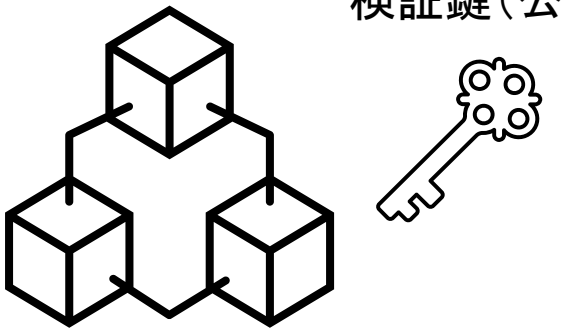


わるいひと

そうきんしゃ

もし、署名鍵を奪われてしまったら、、、

検証鍵（公開）



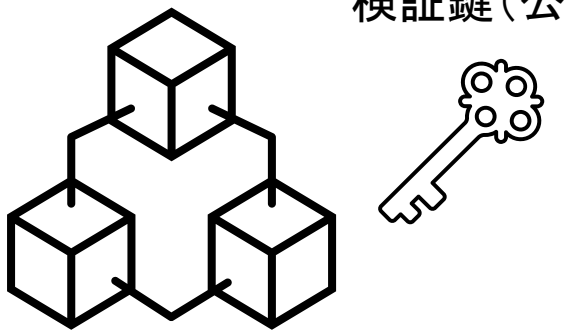
そうきんしゃくんの
署名鍵（秘密）

わるいひと

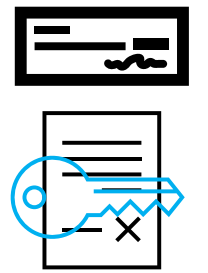
そうきんしゃ

もし、署名鍵を奪われてしまったら、、、

検証鍵（公開）



そうきんしゃくんの
署名鍵（秘密）

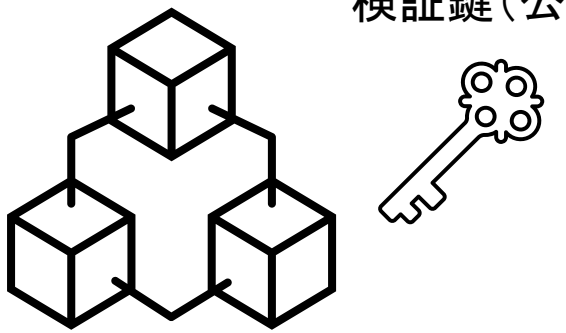


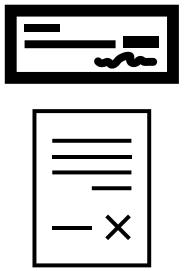
わるいひと

そうきんしゃ

もし、署名鍵を奪われてしまったら、、、

検証鍵（公開）





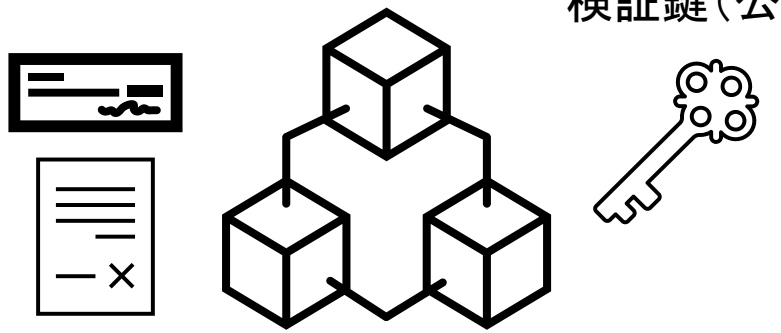
そうきんしゃくんの
署名鍵（秘密）

わるいひと

そうきんしゃ

もし、署名鍵を奪われてしまったら、、、

検証鍵（公開）

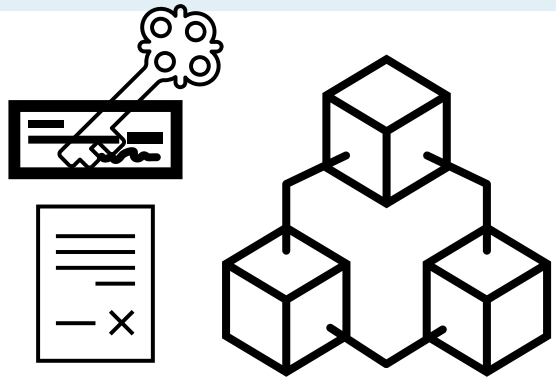


そうきんしゃくんの
署名鍵（秘密）

わるいひと

そうきんしゃ

もし、署名鍵を奪われてしまったら、、、



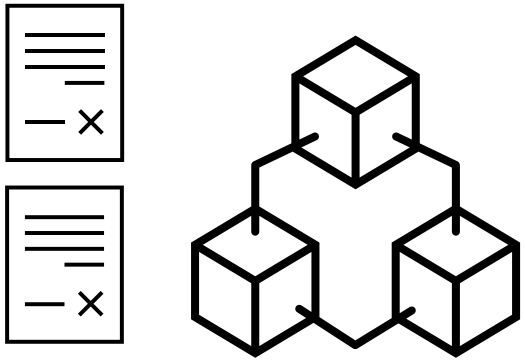
検証鍵（公開）

そうきんしゃくんの
署名鍵（秘密）

わるいひと

そうきんしゃ

もし、署名鍵を奪われてしまったら、、、



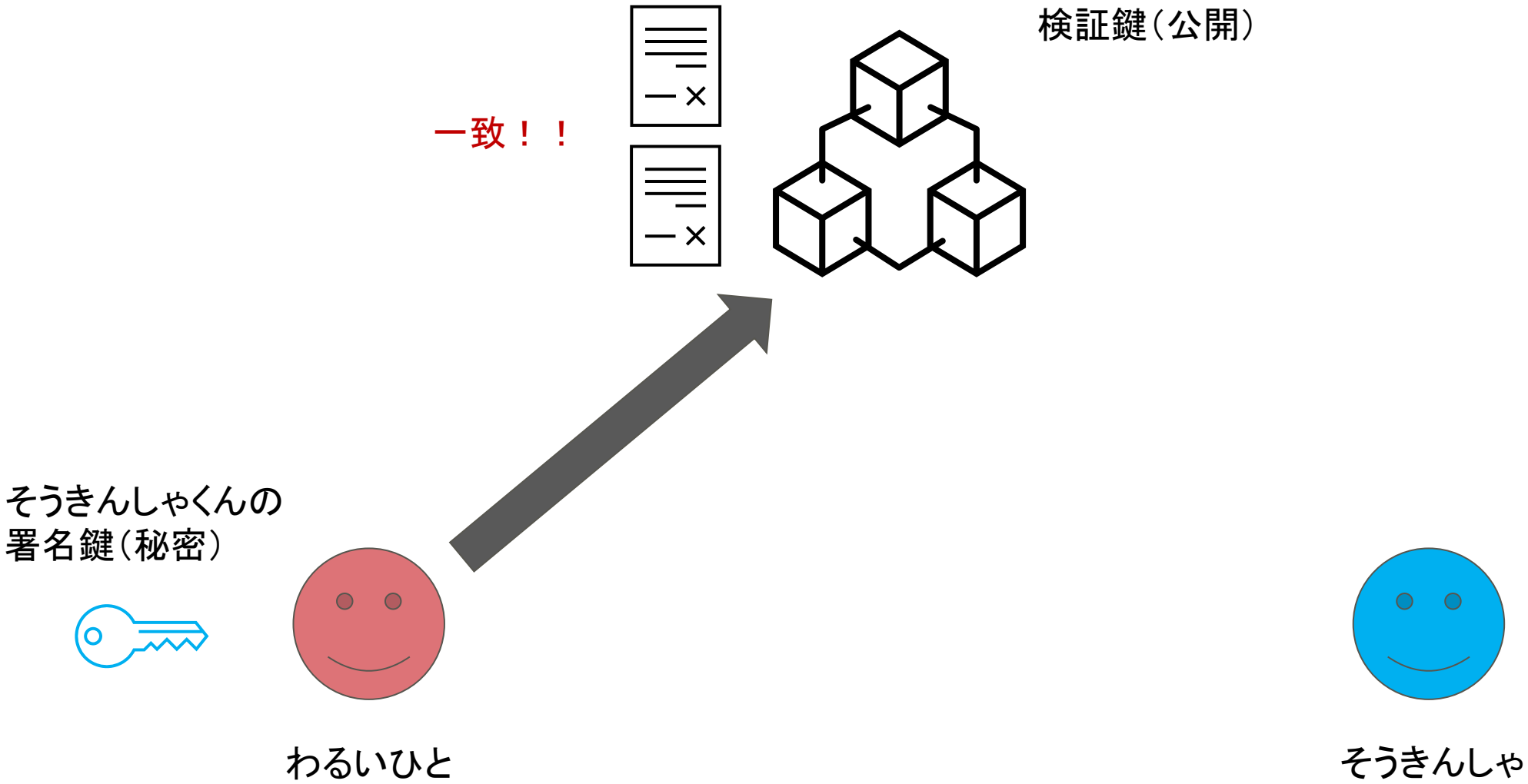
検証鍵（公開）

そうきんしゃくんの
署名鍵（秘密）

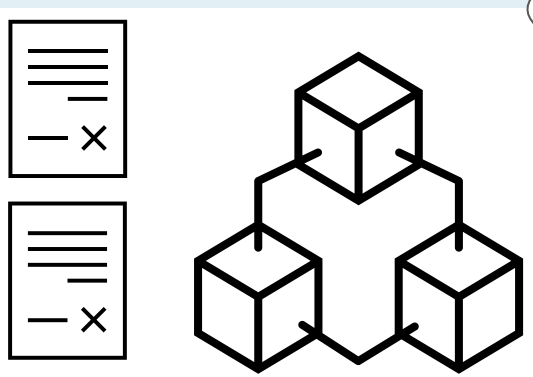
わるいひと

そうきんしゃ

もし、署名鍵を奪われてしまったら、、、



もし、署名鍵を奪われてしまったら、、、



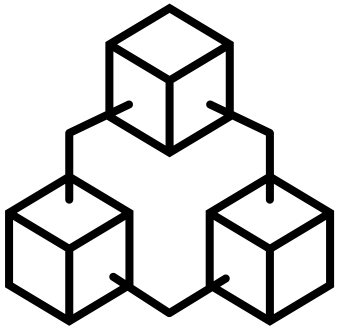
これはそうきんしゃくんが作った
トランザクションだから問題ナシ！承認！

そうきんしゃくんの
署名鍵（秘密）

わるいひと

そうきんしゃ

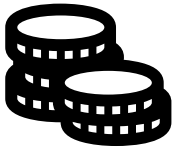
もし、署名鍵を奪われてしまったら、、、



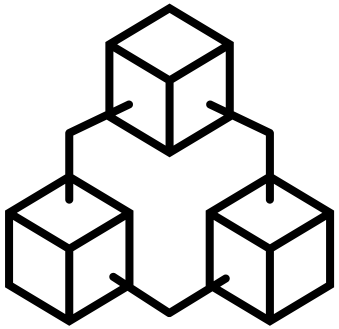
そうきんしゃくんの
署名鍵（秘密）

わるいひと

そうきんしゃ

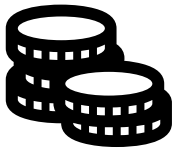


もし、署名鍵を奪われてしまったら、、、



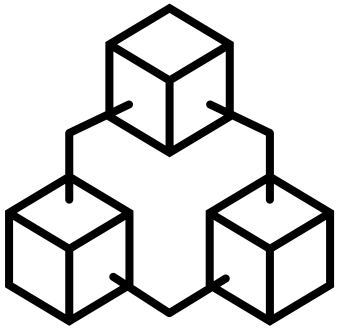
そうきんしゃくんの
署名鍵（秘密）

わるいひと



そうきんしゃ

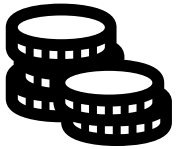
もし、署名鍵を奪われてしまったら、、、



お金を奪えた！！

そうきんしゃくんの
署名鍵（秘密）

わるいひと



お金を奪われた！！

そうきんしゃ

もし、署名鍵を奪われてしまったら、、、

つまり、電子署名を用いても、署名鍵が取られてしまうと
不正な取引が承認されてしまう。

よって、署名鍵の管理・保管が重要な問題である。

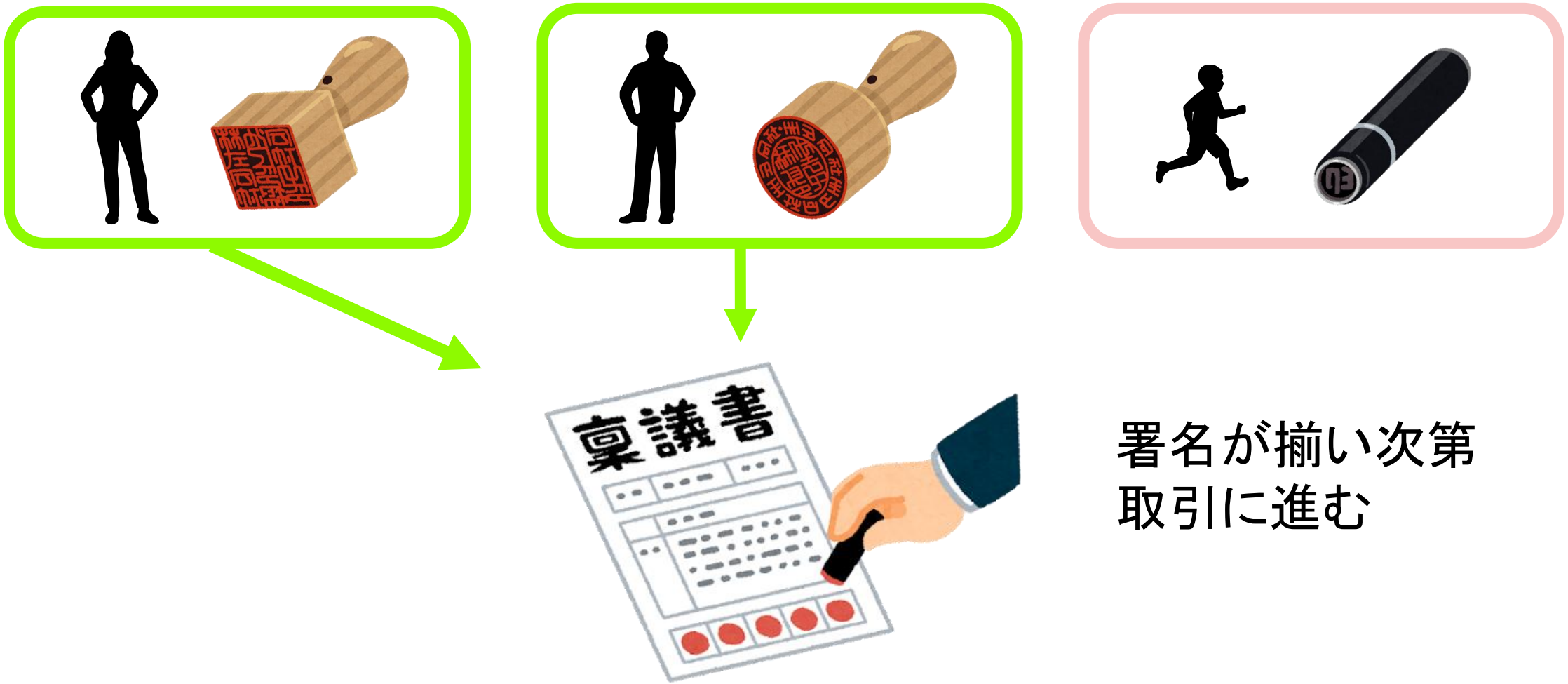
この鍵管理問題が、本課題の根本的な問題である。

マルチシグ(Multi-sig)に対するしきい値t/nの最適設計

著者）
山崎 拓己（九州大学大学院マス・フォア・イノベーション連係学府）
安田 渓（九州大学大学院マス・フォア・イノベーション連係学府）
宮崎 雅哉（九州大学大学院マス・フォア・イノベーション連係学府）
川西 晴貴（九州大学大学院数理学府）

マルチシグの例(2 out of 3)

2 out of 3 では3つのハンコのうち2つでの署名が必要



署名が揃い次第
取引に進む

マルチシグの安全性

安全性

1. 署名鍵のない人がウォレットから送金できない
2. 複数人で管理するときに総意が反映される

鍵の盗難確率:p

ウォレットの盗難確率:$P(t,n) = \sum_{k=t}^{n} \binom{n}{k} p^k (1-p)^{n-k}$　改善率:$\frac{P(t,n)}{p}$

資産に対するウォレットの金額の割合(M),
資産に対する損失許容金額の割合(N),
必要改善率: $S = \frac{N}{M*p}$

$\frac{P(t,n)}{p} \leq S$　安全性を満たすと仮定する。

マルチシグの安全性

安全性

1. 署名鍵のない人がウォレットから送金できない
2. 複数人で管理するときに総意が反映される

鍵の盗難確率:p

ウォレットの盗難確率:$P(t,n) = \sum_{k=t}^{n} \binom{n}{k} p^k (1-p)^{n-k}$　改善率:$\frac{P(t,n)}{p}$

資産に対するウォレットの金額の割合(M),
資産に対する損失許容金額の割合(N),
必要改善率: $S = \frac{N}{M*p}$

$\frac{P(t,n)}{p} \leq S$　安全性を満たすと仮定する。

マルチシグの安全性

安全性

1. 署名鍵のない人がウォレットから送金できない
2. 複数人で管理するときに総意が反映される

n人、n個の鍵でウォレットを管理するときt人の意志が合致で
ウォレットの送金が可能

選択肢が2択のとき全体の総意が正しく反映されるのは多数決

tはnの過半数の最小の値が必要　$t = \left\lceil \frac{n}{2} \right\rceil + 1$

マルチシグの可用性

鍵を紛失してもマルチシグが可能か？

t out of n の時、$n - t$本鍵を紛失してもマルチシグは可能

n-tを最大化するのが可用性

課題解決の流れ

以下の2つの場合に分けて安全性、可用性を考えた時に最適な閾値t/nを見つける

1. 個人ウォレット・・・一人で1つのウォレットを管理

2. 共同ウォレット・・・複数人で1つのウォレットを管理

1：個人ウォレットの最適な閾値

評価方法

現在、一人で持つ鍵の個数は多くても5個なのでn≦5を考えればよい

鍵盗難確率p= (2025年度ウォレット被害件数/2025年度アクティブユーザー数)と定義する。

この時 $P(t,n)$とSを計算して

$\frac{P(t,n)}{p} \leq S$ を満たすnに対する最小のtを見つければ良い

評価

ウォレットの金額が資産の20%と仮定し、資産の0.01%の損失なら許容できるとする。

この時の必要改善率は$S = \frac{N}{M*p} = \frac{0.001}{0.2*0.005} = 0.1$ となる

$t \geq 2$なら$\frac{P(t,n)}{p} \leq S$ を満たす。可用性からtは最小値を取ればよい。

よって個人の場合は2/3、2/4、2/5が最適である。

2：共同ウォレットの最適な閾値

評価方法

現在、共同ウォレットで使われている鍵の個数は多くても10個
n≦10を考えれば良い

鍵盗難確率p= (2025年度ウォレット被害件数/2025年度アクティブユーザー数)と定義する。

この時P(t,n)とSを計算して
$\frac{P(t,n)}{p} \leq S$ を満たすnに対する最小のtを見つければ良い

複数人での利用は、全体の総意が反映されるかが重要
$t \geq \left\lceil \frac{n}{2} \right\rceil + 1$を考えれば良い

評価

ウォレットの金額が資産の100%と仮定し、資産の0.01%の損失なら許容できるとする。

この時の必要改善率はS=$\frac{N}{M*p} = \frac{0.0001}{0.005} = 0.02$ となる

この時$t \geq \left\lceil \frac{n}{2} \right\rceil + 1$すべての時 $\frac{P(t,n)}{p} \leq S$ を満たす。

よってt= $\left\lceil \frac{n}{2} \right\rceil + 1$が最適

まとめ

まとめ

・一人で一つのウォレットを使うとき

n≦5に対してt=2が最適

・複数人で一つのウォレットを使うとき

n≦10に対して現在よく使われているt= $\left\lceil \frac{n}{2} \right\rceil + 1$が最適

しきい値 t/n の最適設計

著者）
金重 幸大（九州大学大学院マス・フォア・イノベーション連係学府）
朝重 菜音（九州大学大学院マス・フォア・イノベーション連係学府）
村上 真悟（九州大学大学院マス・フォア・イノベーション連係学府）
寺本 優斗（九州大学大学院数理学府）
堂後 航希（九州大学大学院数理学府）

目次

- 取り組みの流れ
- 問題設定
- 成果
- 今後の課題

取り組みの流れ

- アプローチa
  - ✓ 機械学習を用いて最適なしきい値(t, n)を決めることができる評価関数の作成を行う。

    but…必要となるデータセットが公開されていないため断念

- アプローチb
  - ✓ 安全性や可用性について閾値を決める値(t, n)を入力に含む関数で定義する。

    →出力が嬉しくなる(t, n)を探す。

- アプローチbでの成果を発表する。

問題設定

- 可用性＝「ユーザー視点の使い心地」を表す指標
- 安全性＝「攻撃者による不正の受けにくさ」を表す指標
- 可用性と安全性にはトレードオフの関係がある

ちょっと待って！！

数式的な定義がない！！

問題設定

- 可用性＝「ユーザー視点の使い心地」を表す指標
- 安全性＝「攻撃者による不正の受けにくさ」を表す指標
- 状況に応じて次のような変化をするように指標を定めたい

状況	可用性	安全性
承認に要する時間　短	↑	
ネットワーク障害耐性　高	↑	
しきい値t　高	↓	↑
バックアップ数　多	↑	↓

- 入力として想定した主なパラメータ
  - ✓ 利用者がオンラインになる確率
  - ✓ 各個人の平均した鍵侵害確率と鍵紛失確率
  - ✓ 平均のバックアップ数
  - ✓ ネットワークのつながりや鍵の分散状況を表すグラフ

成果1(可用性について)

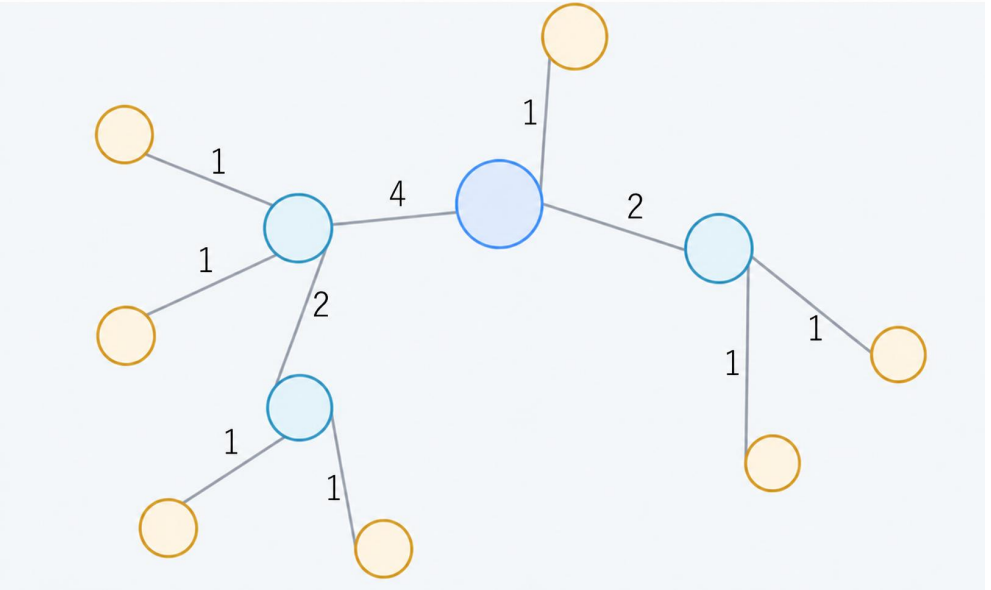
- 可用性を表す式

$$\sum_{m=t}^{n}\sum_{i=t}^{m}\binom{n}{m}\binom{m}{i}q^{m}(1-q)^{n-m}p^{i}(1-p)^{m-i}$$ + グラフの評価値の項

  - ✓ t: しきい値t/nのt
  - ✓ n: しきい値t/nのn
  - ✓ q: 鍵を侵害されていない割合
  - ✓ T: 署名の要求がされてからの経過時間
  - ✓ $p = p(T) = 1 - e^{-\lambda(b)T}$: 時刻Tまでにオンラインになる確率
  - ✓ b: 一人当たりが持つ鍵の平均本数
  - ✓ $\lambda(b) = \lambda_0 + 1/(1 + e^{-a(b+1)})$: オンラインパラメータ

- この式の値が大きいほど可用性が高いと考える。

グラフの例（インターネット構造の評価）



成果2(安全性について)

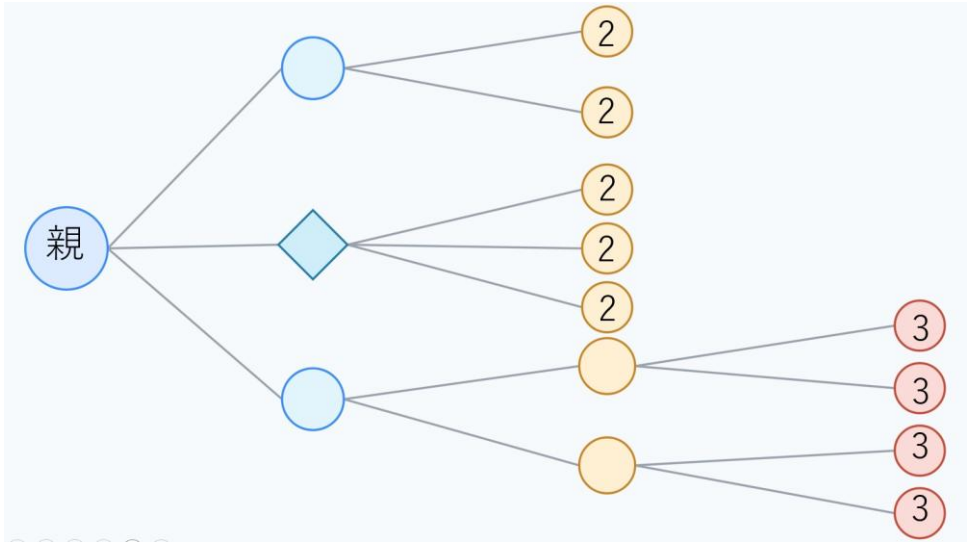
- 安全性を表す式

$$1-\sum_{m=t}^{n}\binom{n}{m}\left(1-(1-s)^{b}\right)^{m}(1-s)^{b(n-m)} + \text{グラフの評価値の項}$$

  - ✓ t : しきい値t/nのt
  - ✓ n: しきい値t/nのt
  - ✓ s : 鍵侵害確率
  - ✓ b : 一人当たりが持つ鍵の平均本数

- この式の値が大きいほど安全性が高いと考える。

グラフの例（鍵分散の評価）



今後の課題

- 実データに基づいた係数の設定

- データセットの充実化
  - ✓ 回線の断線確率
  - ✓ オンライン確率
  - ✓ 鍵侵害確率

  etc…

- 今回定義した可用性・安全性を考慮した署名方式の選択

- 耐量子性を組み込んだ安全性の再定義

ホット・コールド分布の最適化

著者）
山崎 拓己（九州大学大学院マス・フォア・イノベーション連係学府）
安田 渓（九州大学大学院マス・フォア・イノベーション連係学府）
宮崎 雅哉（九州大学大学院マス・フォア・イノベーション連係学府）
川西 晴貴（九州大学大学院数理学府）

1）ホット・コールド分布の最適化

対象：暗号資産交換業者

（Coincheck　SBI VCトレードなど）

→ 暗号資産の取り扱いには二つの方法がある

ホットウォレット・・・インターネットに接続された状態で、鍵を管理

✓メリット：送金、取引が早い

✓デメリット：セキュリティリスク高

コールドウォレット・・・オフライン上で鍵を管理

✓メリット：セキュリティリスク低

✓デメリット：送金、取引に時間がかかる

→ この最適なバランスを探りたい

総預かり資産の運用ルール（我々の設定）

- 開始時点の総預かり資産　$M_0 = 6050$億円 (とある企業の2025年の資産に相当)
- 半日当たりの出金額の分布

  80%で3.025億円　19%で15.125億円　　1%で60.5億円
- 計測期間1年（半日×730）
- ホットウォレットの上限n_1%, 下限n_2%を設定

  ホットH ←$M_0 \times n_1$　#本当は100で割る必要があるが省略

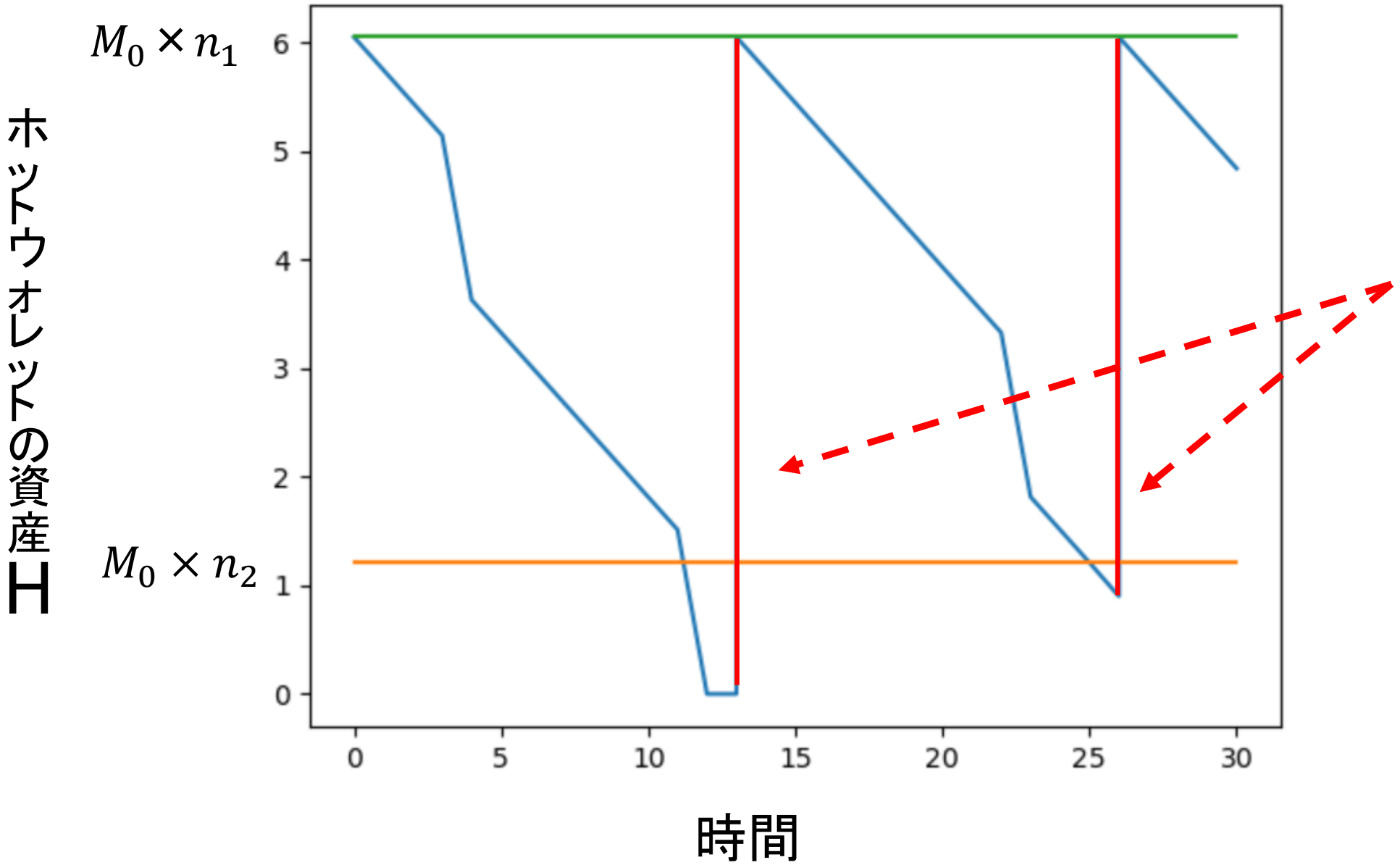
  for i in range(730):

    H ← H −（80%で3.025億円、19%で15.125億円、1%で60.5億円）

    if H ≤ $M_0 \times n_2$:

      H ← $M_0 \times n_1$ #下限を下回ったら、ホットウォレットを補充

イメージ図①


$M_0 \times n_1$
$M_0 \times n_2$
ホットウォレットの資産H
0
1
2
3
4
5
6
0
5
10
15
20
25
30
時間
$M \times n_2$
を下回るごとに
補充が発生

評価方法1/4

- 企業はこのモデルの元、3つのリスクとコスト(R,W,L)を負う
  リスクの期待値とコストを合わせて損失と言う

①ホットウォレット資産の盗難リスク（R＝盗難リスク）

- 半日あたりの鍵侵害確率をp=1.6537×10^{-5}と設定

ホットH ←$M_0 \times n_1$

R＝0

for i in range(730):

H ← H −（80%で3.025億円、19%で15.125億円、1%で60.5億円）

R＝R＋H×p　#半日ごとの盗難期待値を足していく

if H ≤ $M_0 \times n_2$:

H ← $M_0 \times n_1$

評価方法2/4

②コールド→ホット移動のリスクとコスト（W＝移動損失）

移動1回当たりコスト:　5万

移動1回当たりのリスクの期待値:　(移動金額)$\times 10^{-5} + M_0 \times 10^{-6}$

ホットH ← $M_0 \times n_1$

W=0

for i in range(730):

H ← H −（80%で3.025億円、19%で15.125億円、1%で60.5億円）

if H ≤ $M_0 \times n_2$:

W = W+50000+$(M_0 \times n_1 - \mathrm{H}) \times 10^{-5} + M_0 \times 10^{-6}$

#補充が発生するごとにその損失を足していく

H ← $M_0 \times n_1$

評価方法3/4

③ホットウォレットの金額不足によるリスクとコスト（L＝不足損失）

- 1回当たりの損失：100万＋(不足額)×10^{-2}

ホットH ←$M_0 \times n_1$

L=0

for i in range(730):

H ← H −（80%で3.025億円、19%で15.125億円、1%で60.5億円）

if H ≤ $M_0 \times n_2$:

if H < 0:

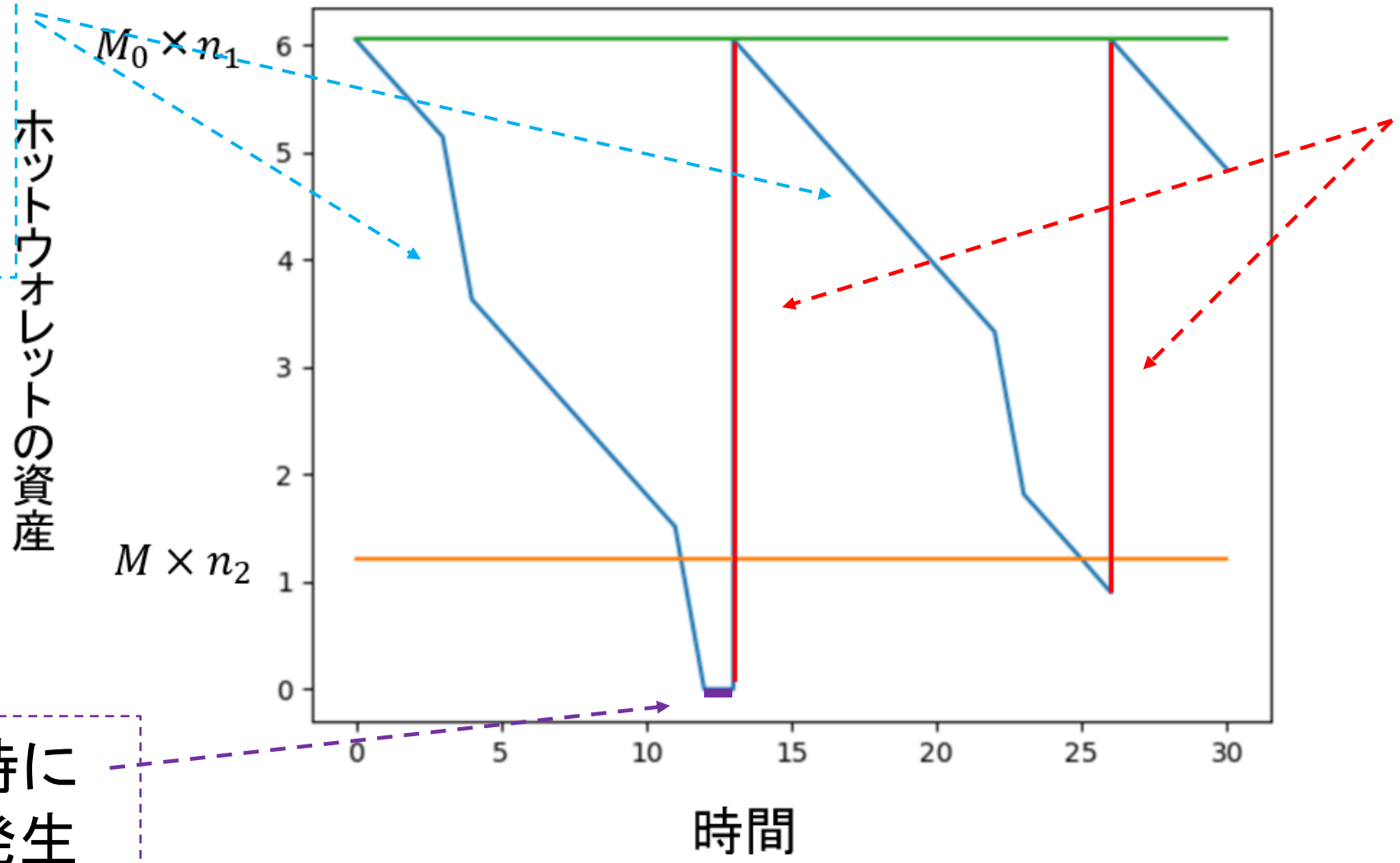
L = L+100万−(H×10^{-2})

#費用が不足するごとに、その損失を足していく

H ← $M_0 \times n_1$

イメージ図②

盗難リスクRはグラフが平均的に上にあるほど大きい



補充ごとに損失Lが発生

不足した時に損失Hが発生

評価方法4/4

- R,W,Lは半日あたりの出金額と、n_1, n_2によって決まる

総損失額＝R＋W＋Lが最小となるn_1, n_2を見つけたい

$0\% \leq n_2 < n_1 \leq 5\%$ (0.1刻み）で実験を行った

実験結果

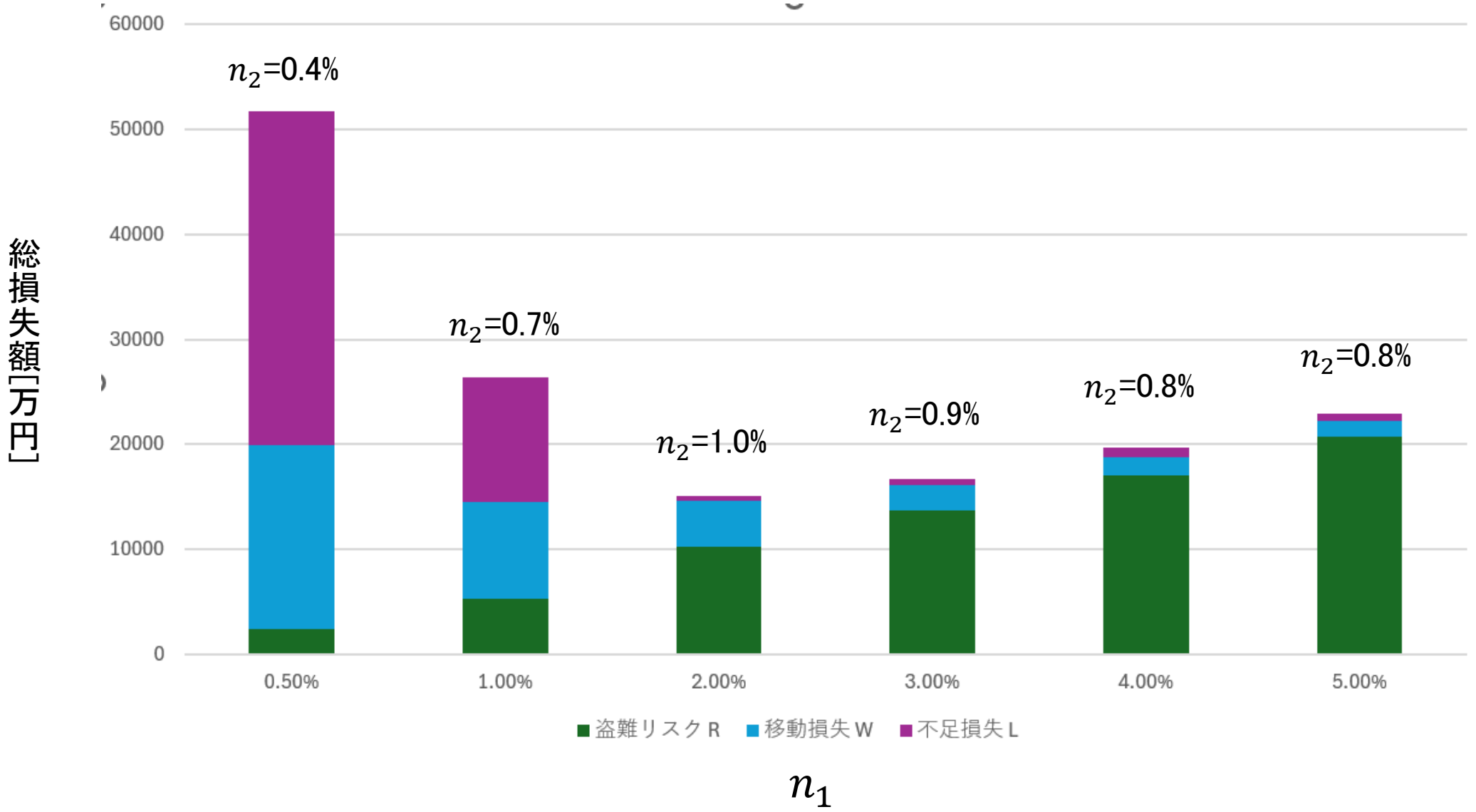
- n_1=2.0%、n_2=1.0%がコスト最小

上位結果5個（桁は万円）

n1	n2	盗難リスク R	移動損失 W	不足損失 L	総損失額 R+W+L	最小値との差
2.00%	1.00%	10,305	4,298	539	15,142	0.00%
2.10%	1.00%	10,682	4,001	530	15,213	0.47%
1.90%	1.00%	9,743	4,468	1,008	15,219	0.51%
2.00%	0.90%	9,954	3,995	1,308	15,258	0.76%
2.10%	0.90%	10,329	3,740	1,216	15,285	0.94%

n_1は最適の2.0を中心に、1.9～2.1付近に最適解が分布
n_2はそれより許容幅が狭く、基本1.0～0.9が最適となる

n_1のトレードオフ分析(n_2は各n_1に対し最適な値とする)



パラメータ変更による、最適値の変化

- 標準モデルからパラメータを変更し、最適n_1, n_2の変化を実験

モデル	変更した仮定	変更量	最適n1	最適n2
基本モデル	なし	なし	2.00%	1.00%
鍵侵害確率大モデル	年鍵侵害確率	1.2%→2.0%	1.75%	1.00%
鍵侵害確率小モデル	年鍵侵害確率	1.2%→0.2%	4.00%	1.00%
顧客要求大モデル	顧客要求額	基本の2.0倍	3.25%	2.00%
顧客要求小モデル	顧客要求額	基本の0.5倍	1.25%	0.50%

考察：鍵侵害確率が高いほど、n_1は低い方が有利
またn_2は顧客要求に比例する形で最適値が決定

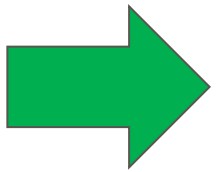
成果とまとめ

- 各種パラメータとn_1, n_2に対し企業の総損失額を

「移動損失」「不足損失」「盗難リスク」の3要素から推察するアルゴリズムを作成

- 実験を行い、最適な上限、下限を特定

$$n_1=2.0\%,\ n_2=1.0\%$$



金融庁の課す、ホットウォレット上限5%の下
企業は十分最適な運用ができる

- 設定パラメータを変更することで、n_1, n_2の最適値がどう変化するかを調べた

補足資料(可用性の実験結果)

- 可用性の計算結果例

$$\sum_{m=t}^{n}\sum_{i=t}^{m}\binom{n}{m}\binom{m}{i}q^{m}(1-q)^{n-m}p^{i}(1-p)^{m-i}$$

n	t=1	t=2	t=3	t=4	t=5	t=6	t=7	t=8
2	0.8960	–	–	–	–	–	–	–
3	0.9665	0.7551	–	–	–	–	–	–
4	0.9892	0.8983	0.6119	–	–	–	–	–
5	0.9965	0.9599	0.8060	0.4826	–	–	–	–
6	0.9989	0.9847	0.9103	0.7017	0.3730	–	–	–
7	0.9996	0.9943	0.9607	0.8430	0.5957	0.2839	–	–
8	0.9999	0.9979	0.9835	0.9228	0.7633	0.4952	0.2135	–
9	1.0000	0.9992	0.9933	0.9639	0.8713	0.6768	0.4044	0.1590

- t: しきい値t/nのt
- n: しきい値t/nのn
- q: 鍵を侵害されていない割合
- $p = p(T) = 1 - e^{-\lambda(b)T}$: 時刻Tまでにオンラインになる確率
- $\lambda(b) = \lambda_0 + 1/(1 + e^{-a(b+1)})$: オンラインパラメータ

係数設定

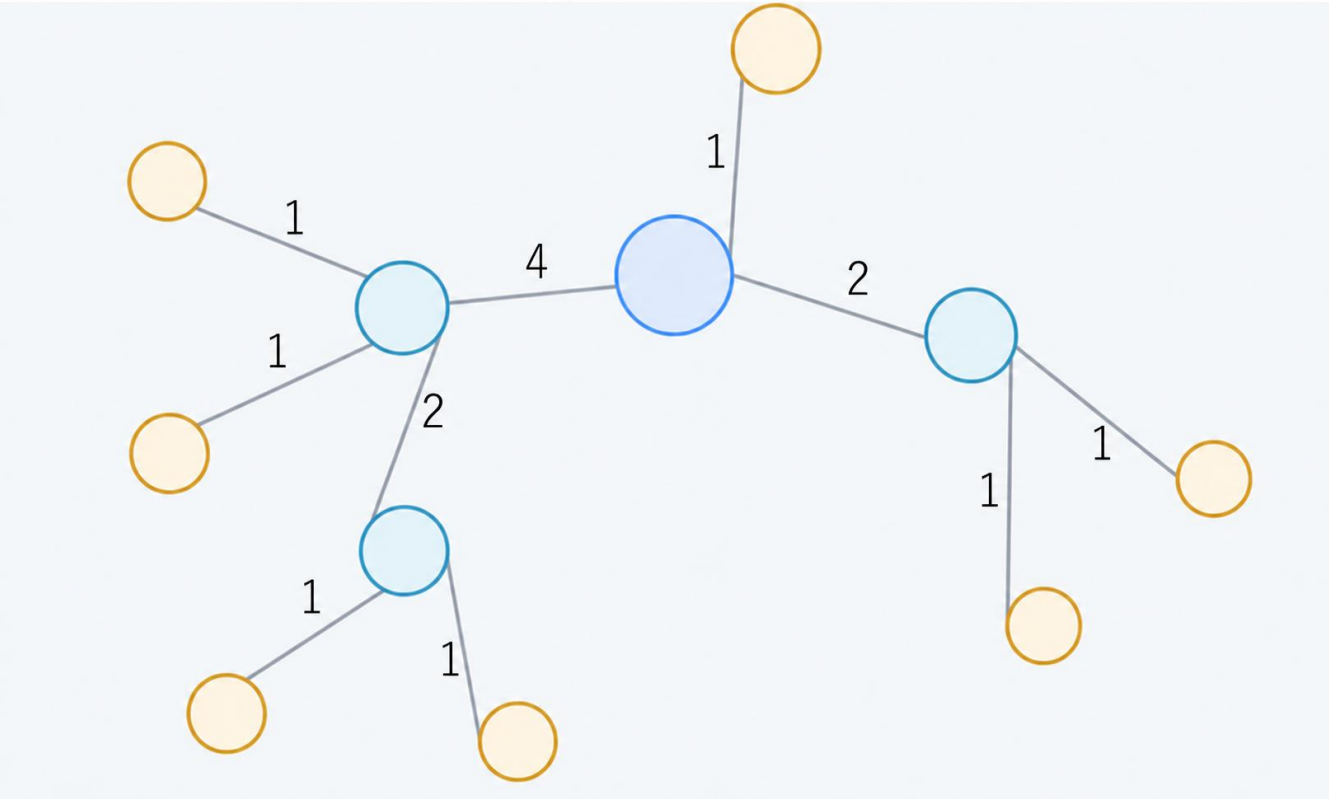
$q = 0.95$

$p(20) = 0.713$

$\lambda(2) = 0.062$

補足資料（グラフの評価値の例）

グラフの例（インターネット構造の評価）



- 末端ノード数が多い中継地点
→リスクが集中しており危険

- 今回理想状態と考えたグラフの評価値は0になる

- 左のグラフの評価値は $\frac{24}{31}$

グラフの評価値＝１－（末端ノード数/辺の評価値の2乗和）